



**EMERGING ROLES OF COMBAT COMMUNICATION SQUADRONS
IN CYBER WARFARE
AS RELATED TO
COMPUTER NETWORK ATTACK, DEFENSE AND EXPLOITATION**

GRADUATE RESEARCH PROJECT

Michael J. Myers, Major, USAF

AFIT/ICW/ENG/11-10

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

The views expressed in this report are those of the author and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

AFIT/ICW/ENG/11-10

EMERGING ROLES OF COMBAT COMMUNICATION SQUADRONS
IN CYBER WARFARE
AS RELATED TO
COMPUTER NETWORK ATTACK, DEFENSE AND EXPLOITATION

GRADUATE RESEARCH PROJECT

Presented to the Faculty
Department of Electrical and Computer Engineering
Graduate School of Engineering and Management
Air Force Institute of Technology
Air University
Air Education and Training Command
In Partial Fulfillment of the Requirements for the
Degree of Master of Cyber Warfare

Michael J. Myers
Major, USAF

June 2011

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

EMERGING ROLES OF COMBAT COMMUNICATION SQUADRONS
IN CYBER WARFARE
AS RELATED TO
COMPUTER NETWORK ATTACK, DEFENSE AND EXPLOITATION

Michael J. Myers
Major, USAF

Approved:

/signed/

1 Jun 2011

Michael R. Grimaila, PhD, CISM, CISSP
(Chairman)

date

/signed/

1 Jun 2011

Kenneth Hopkinson, PhD (Member)

date

Abstract

The warfighter has become increasingly dependent of the cyber domain and the computer network the deployed forces use to plan and execute the Commander's intent to accomplish the objectives for mission success. There is a growing intensity to defend the warfighter's mission that is dependent on the network, instead of defending the entire Air Force Global Information Grid (GIG). This full spectrum of cyber dominance must include the need for computer network attack, defense and exploitation (CNA/D/E) at the tactical level.

The dilemma at hand, involves two distinct solutions on how to achieve input at the tactical level to ensure mission assurance for the commander. The solutions presented are to either one, rely on external remote resources or two, to have a trained force on-site in the area of responsibility (AOR) that can perform the same CNA/D/E actions. This research intends to show how the latter solution performed by an Air Force Combat Communications Squadron (CCS) can provide those complete cyber capabilities needed for a deployed force commander to obtain full mission assurance in the cyber domain.

The CCSs are the Air Force's deployable communication force structure for the joint and coalition warfighter during combat and Humanitarian Relief Operations. The CCS's core competencies must continue to move from network assurance to mission assurance in a tactical communication environment. To achieve this, the CCS mission should strive to balance bare-base operations and reshape their mission to include CNA/D/E capabilities to evolve combat communication squadrons into a total cyber force tactical unit.

The focus of this research explores this need for the CCS to provide this new mission capability on-site for the deployed commander's employment. This research

concludes by expanding and building upon similar Air Force unit team compositions for the CCS to adopt with a time-phased implementation plan.

Acknowledgements

I would like to express my sincere appreciation to my research advisor, Dr. Michael Grimaila, for his guidance and support throughout the course of this effort. The insight and experience was certainly appreciated.

Additionally, I wish to thank Col Theresa Giorlando, the Commander, of the 689 Combat Communications Wing for her GRP sponsorship, her mentorship, thoughtful interview insights and support in distributing the survey created for this research.

I would also like to thank Maj Gen Capasso for his support and endorsement of the survey and the other three interviewees, Brig Gen Earl Matthews, Col Von Gardiner and Col Robert Skinner. Thanks also goes to Mr. Sampson who provided the technical work for the on-line survey and for all the survey participants who took the time to share their experiences and thoughts. I am grateful for everyone's support.

I am also indebted to the many professionals and friends who provided insight and suggestions and encouragement as I endeavored to complete this project. . . Thank You All

Finally, I want to thank my beautiful dedicated wife, two lovely daughters, and my supportive son, all of which drive me to continually improve myself through persistence, patience and at times, procrastination . . . My family is my ultimate motivation.

Michael J. Myers

Table of Contents

| | Page |
|--|------|
| Abstract | iv |
| Acknowledgements | vi |
| List of Figures | ix |
| List of Tables | xi |
| I. Introduction | 1 |
| II. Background | 4 |
| 2.1 Assumptions | 4 |
| 2.2 Considering Other Options First (DIME) | 4 |
| 2.3 Policy, Rules of Engagement (ROE) and Legal Overview | 5 |
| 2.4 The Role of the “6” Community to the Commander | 7 |
| 2.5 Cyberspace Defined | 8 |
| 2.6 Network Assurance and Mission Assurance Defined | 9 |
| III. Building the Case: Tactical Success Enables Mission Assurance | 12 |
| 3.1 Mission Assurance at the Tactical Level | 12 |
| 3.2 Moving from Network Assurance to Mission Assurance | 14 |
| 3.3 Participation at the Tactical Level: Two Options | 16 |
| IV. Respondent Survey Statistics and Interviews | 18 |
| 4.1 Survey Overview | 18 |
| 4.2 Target Audience | 19 |
| 4.3 Respondent Statistics | 19 |
| 4.3.1 Statistics Overview | 19 |
| 4.3.2 Current/Recent Deployed Capabilities and Experiences | 19 |
| 4.3.3 Viewpoints on Needed On-site CNA/D/E Capabilities | 23 |
| 4.4 Interviews | 32 |
| 4.4.1 Air Force Special Operations (AFSOC) A6 | 32 |
| 4.4.2 US Transportation Command (USTRANSCOM) J6 | 35 |
| 4.4.3 688th Information Operations Wing (IOW) Commander | 35 |
| 4.4.4 689th Combat Communications Wing (CCW) Commander | 37 |

| | Page |
|---|------|
| V. Survey and Interview Analysis and Recommendations | 40 |
| 5.1 Preparing a Combat Communication Squadron for this New Mission | 40 |
| 5.1.1 Policy and Legal Concerns | 40 |
| 5.1.2 Training Concerns | 41 |
| 5.1.3 Current Structure | 44 |
| 5.1.4 Proposed Structure | 44 |
| 5.1.5 Proposed Tool Sets | 50 |
| 5.1.6 Time Phased Implementation | 54 |
| 5.2 Final Thoughts and Challenges | 55 |
| VI. Conclusions | 57 |
| Bibliography | 59 |
| Appendix A. Interviewee’s Public Release Statements | 62 |
| A.1 Col Giorlando’s Interview Release Statement | 62 |
| A.2 Col Gardiner’s Interview Release Statement | 63 |
| A.3 Col Skinner’s Interview Release Statement | 64 |
| A.4 Gen Matthew’s Interview Release Statement | 65 |
| Appendix B. Survey Questions | 66 |
| Appendix C. Referenced Unit Mission Descriptions | 71 |
| Appendix D. Researcher’s Vita | 75 |

List of Figures

| Figure | | Page |
|--------|--|------|
| 1 | Ranks of All Respondents | 20 |
| 2 | Deployed Respondents | 20 |
| 3 | Ranks of Deployed Respondents | 21 |
| 4 | Deployed Unit Supported the Commander in the Following Capacity | 21 |
| 5 | Deployed Unit <i>Should Have</i> Supported the Commander in the Following Capacity | 22 |
| 6 | Barriers Why Unit <i>Did Not</i> Support Commander While Deployed | 23 |
| 7 | Deployed Commander <i>Should have</i> an On-site Tactical CNA/D/E Capability | 24 |
| 8 | Rationale <i>Against</i> an On-site Tactical CNA/D/E Capability . . | 25 |
| 9 | Active Duty Ranks of Military Respondents <i>Against</i> an On-site Tactical CNA/D/E Capability | 26 |
| 10 | Active Duty Respondents <i>Against</i> an On-site Tactical CNA/D/E Capability | 26 |
| 11 | Barriers to an On-site Tactical CNA/D/E Capability | 27 |
| 12 | Active Duty Ranks of Military Respondents <i>For</i> an On-site Tactical CNA/D/E Capability | 28 |
| 13 | Retired Ranks of Military Respondents <i>For</i> an On-site Tactical CNA/D/E Capability | 28 |
| 14 | Active Duty Respondents <i>For</i> an On-site Tactical CNA/D/E Capability | 30 |
| 15 | Total Respondents who believe it <i>IS or IS NOT</i> necessary to have an On-site Tactical CNA/D/E Capability | 30 |
| 16 | Percent of Responses who believe it <i>IS or IS NOT</i> necessary to have an On-site Tactical CNA/D/E Capability | 31 |
| 17 | Percent of Respondents who believe it <i>IS or IS NOT</i> necessary to have an On-site Tactical CNA/D/E Capability | 31 |

| Figure | | Page |
|--------|---|------|
| 18 | United States Code Legal Authorities within 24 AF [1] | 41 |
| 19 | 24th Air Force Structure [1] | 45 |
| 20 | Hunter Team Composition [2] | 46 |
| 21 | CCS Hunter Team Composition | 48 |
| 22 | CCS Cyber Hunt & Kill Team Composition | 50 |
| 23 | Geographic Distribution of Stuxnet Infections [3] | 51 |
| 24 | 24 AF Joint C2 Relationships [1] | 53 |

List of Tables

| Table | | Page |
|-------|---|------|
| 1 | Mission Assurance and Network Assurance Relations | 14 |

EMERGING ROLES OF COMBAT COMMUNICATION SQUADRONS
IN CYBER WARFARE
AS RELATED TO
COMPUTER NETWORK ATTACK, DEFENSE AND EXPLOITATION

I. Introduction

In today's military environment, there are different military services that bring different capabilities to bear in times of conflict, in times of natural or man-made disasters, in times the child's voice cries for a champion against human suffering. It is in these times that America's military services (and the nation's partners) come together in a joint endeavor to overcome the atrocity and/or affliction. During any large-scale operation it is about effective communication that avoids chaos and focuses efforts for maximum mission success. Effective communication is the basis for successful command and control (C2); providing leaders the eyes and ears for situational awareness (SA) and the avenue for a commander's "voice projection" to command the unity of effort for all activities necessary for mission success. This is why joint communications, in the sense of Joint Operations, lay at the heart of a well executed operation and results in mission success ... the goal of mission assurance ... success.

To effectively support the overall Joint Force Commander's (JFC's) mission, either deployed in another country or, if needed here in America, the communication element supporting that mission must change focus from network assurance to mission assurance to enable seamless, effective and efficient C2. This transformation should occur at all levels of operations (strategic, operational and tactical), but this research addresses leveraging this change in focus at the tactical communication level to allow for inherent success of the higher levels.

As cyber professionals it is not about just providing a service for the customers, the warfighters, but ensuring their missions that rely upon the cyber domain for their

execution prevail under any circumstance. It is important not to forget that the fight is won at the tactical level, given other instruments of national power have not persuaded the adversary, before the warfighter can declare operational and strategic victory. Therefore, it only makes sense that mission assurance at the lowest possible denominator must be achieved and maintained for true mission success. Through the employment of the full spectrum of Cyber capabilities (computer network attack (CNA), computer network defense (CND) and computer network exploitation (CNE)), the commander can depend on their network as a force provider and even choice of tools to achieve various non-kinetic (and sometimes kinetic) courses of action (COAs). Currently, the JFC does not have this capability available on-site for employment.

RESEARCH OBJECTIVE

The focus of this research is to examine the potential for the traditional Combat Communication Squadrons (CCS) to expand their capability to include CNA, CND and CNE (CNA/D/E) functions to satisfy this gap in a deployed on-site capability. The research builds upon the continued need to transition from network assurance to mission assurance at the tactical level of warfare and peaceful operations. This research also explores the barriers to employing CNA/D/E at the tactical level required for the commander to achieve mission assurance. The objective of this research is to recommend an achievable and actionable solution for the Air Force to implement to provide this needed on-site CNA/D/E capability for the JFC.

RESEARCH METHODOLOGY

The goals of the research objective are achieved by conducting a survey of communicators and operators with experience in combat communications and/or the planning and execution of various computer network attack, defense and exploitation activities throughout the Air Force and joint operations. Additionally, interviews of key leaders in these same areas are conducted to further explore the relevance of

having this deployed capability for a commander's employment. Finally, an analysis of a similar Air Force construct is examined and built upon as a model framework.

RESEARCH DELIVERABLES

Based upon the analysis of the research, interviews and survey results, recommendations are provided. Specifically, this research concludes with recommendations on how to overcome any real or perceived barriers for CNA, CND and CNE as an on-site capability and expand the cyber capabilities of the combat communication squadron at the tactical edge for the joint force commander with a detailed capability team construct through a time-phased implementation plan.

II. Background

“Today, we forge a long overdue Air Force cultural change. Cyber operations reinforce and enable everything we do - from administrative functions to combat operations - and we must treat our computers and networks similarly to our aircraft, satellites and missiles.”

General Norton Schwartz
Chief of Staff, USAF
27 May 2009

2.1 *Assumptions*

Unless otherwise specified, the term “Commander” refers to the deployed Joint Task Force (JTF) Commander, not the immediate commander of the combat communication squadron. “A [COCOM Commander] normally establishes a subordinate JTF to conduct operations, and forces are normally attached as needed, with specification of operational control (OPCON) to the subordinate Joint Force Commander (JFC). This option will place dedicated [domain] assets and independent command and control (C2) capability under the OPCON of the JFC for whom they are performing the mission.” [4]

2.2 *Considering Other Options First (DIME)*

Before the U.S. President wields his power for military action, most often other techniques are used. These techniques are called the instruments of national power and they are expressed as diplomatic, economic, informational and military and collectively referred to as DIME. Diplomatic powers include bi-lateral and multinational agreements, mutual defense treaties and coalitions. Information powers include intelligence, strategic communications, various media avenues and propaganda campaigns. Economic powers are comprised of sanctions, trade agreements, interest rate manipulations and embargoes against unfavorable nation states. Lastly, the military power is commonly displayed during joint or combined exercises, foreign military sales and exchange programs. But the ultimate display of military might occurs at the time of conflict and use of force to defeat, coerce, dissuade the opposition and reassure

allies of the Nation's commitment. [5], [6] These instruments of national power are described in detail in Joint Publication 1.0. However, even when the Department of Defense (DOD) is supporting a national objective, most often a combination of DIME is employed by the nation to maximize success.

Once the decision to leverage the military might of the United States is made by the President, the military doctrine that outlines the utilization of networks, communications and other electronic exploitations places these capabilities under Information Operations (IO). One of the core competencies in IO is Computer Network Operations (CNO). CNO are used to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure. CNO are divided into Computer Network Attack (CNA), Computer Network Defense (CND), and Computer Network Exploitation (CNE) enabling operations. [7] Specifically, CNA/D/E capabilities are defined as follows:

- Computer network attack (CNA). Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. [7], [8]
- Computer network defense (CND). Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense (DOD) information systems and computer networks. [9], [8]
- Computer network exploitation (CNE). Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. [8]

2.3 Policy, Rules of Engagement (ROE) and Legal Overview

In all military operations, there are defining policies, rules of engagement (ROE) and legal authorities established and followed by forces employed. Policies and ROE tend to be a restraint to operations where laws (legal authorities) are constraints. This is a bit confusing, but a restraint is a device or control that restricts movement

or actions where a constraint is the state of being compelled to avoid or perform some action. For example, to perform an air strike, foreign policy might restraint the use a country's air space, therefore that approach must be avoided. During the air strike there are legal constraints protecting civilian assets, such as hospitals and churches that restrict the targeting of those buildings. Policies are rules and guidelines defined by an organization [DOD]. Laws, on the other hand, are a system of rules established by a governing authority [Congress]. Policy cannot supersede a law. ROEs are policies made that are enforceable by that organization, for example the use of force ROE outlined by DOD.

The 2011 National Military Strategy (NMS) derived from the overarching National Security Strategy document outlines the strategic aims of the armed services and is DOD's key policy guidance. The NMS states that within the cyber domain, [nation] states are "conducting or condoning cyber intrusions that foreshadow the growing threat in this globally connected domain." [10]

The NMS also links the cyberspace capabilities as essential for Combatant Commanders (COCOMS) to achieve successful mission operations across the other domains (air, land, sea and space). The NMS has tasked Strategic Command (USSTRATCOM) and Cyber Command (USCYBERCOM) to "collaborate with U.S. government agencies, non-government entities, industry, and international actors to develop new cyber norms, capabilities, organizations, and skills." [10]

The Quadrennial Defense Review (QDR) is a study by the DOD that analyzes strategic objectives and potential military threats. The QDR recognizes [and charges] DOD to strengthen its capabilities in cyberspace. It states in two [of four] measures to:

- Develop greater cyber expertise and awareness
- Centralize command of cyber operations

[11]

The US Constitution is the bedrock of America’s legal foundation. Through the law-making branch of the US government, the legislative branch enacted derived laws and packaged them into the United States Code (USC) which is further divided into “Titles”. The USC Titles concerning cyber operations and warfare are [12]:

- Title 6 Domestic Security
- Title 10 Armed Forces
- Title 15 Commerce and Trade
- Title 18 Crimes and Criminal Procedure
- Title 32 National Guard
- Title 50 War and National Defense (including Intelligence gathering)

These Titles are pillars of US National law that DOD forces *must* adhere to, however because of the global nature of the Internet and the fact DOD is usually conducting operations outside the US borders, International law is also a concern. Due to the sovereignty of nations, most International law consists of treaties and conventions between nation states. [12]

2.4 The Role of the “6” Community to the Commander

“The objective of the joint communications system is to assist the joint force commander (JFC) in command and control (C2) of military operations. No single activity in military operations is more important than C2.” [9]

The latest technology gadget, largest server, fastest network switch, sleekest webpage or robust database does not guarantee good C2. Effective C2 is founded with well-trained and qualified people, clear objectives and efficient and tested tactics, techniques and procedures (TTPs). To clarify the “6” notation, “6” refers to communications, the codes are commonly associated with different functions in the services, i.e. A6 means communications, A3 means operations. The letter before the number means at which service, i.e. N1 means Navy personnel, A2 means Air

Force Intelligence, J6 means Joint Communications. The J6 assists the commander in all “responsibilities for communications infrastructure, communications-computer networking, communications electronics, information assurance, tactical communications, and interoperability”. [13]

The J6 must provide a “communications system of sufficient scale, accessibility, capacity, reach, and reliability to support evolving operational and training missions” throughout the JFCs area of responsibility (AOR) including reach-back, coalition and other government and/or non-government agency collaboration capabilities. [9] The J6 provides these capabilities to the Commander through the auspices of network operations (NETOPS). NETOPS delivers network SA and end-to-end management of networks, applications, and services while establishing, maintaining, and protecting DODs networks that are a part of cyberspace. [9]

2.5 Cyberspace Defined

There have been plenty attempts to define cyberspace over the past couple of years. In the book Cyber Warfare and Cyber Terrorism, the authors refer to the definition of cyberspace from the Department of Homeland Security’s National Cyberspace Strategy as “the interconnected computers, servers, routers, switches, and cables that make critical infrastructures work.” [14] [15] Martin Libicki, in his Cyberdeterrence and Cyberwar book, defined cyberspace as a virtual medium consisting of a hierarchy of physical, syntactic and semantic layers. [16]. Even in the 2010 AFDD 3-12, Cyberspace Operations publication (pulling from the Joint Publication (JP) 1-02, Department of Defense Dictionary of Military and Associated Terms), has again redefined as it as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.” [17] Regardless of what definition is referenced, cyberspace remains a man-made, global network of operating processors and a seemingly endless

amount of data and information for the warfighter to digest and use towards mission success.

2.6 Network Assurance and Mission Assurance Defined

Only in one DOD document was there a definition for network assurance and it is at the Global Information Grid (GIG) level, but it still applies here. It is defined, in Joint Pub 6.0, as providing end-to-end protection to ensure data quality and protection against unauthorized access and inadvertent damage or modification incorporating: IA protection activities, CND, and critical information protection. [9]

Besides the single instance above, there does not seem to be a standard definition for network assurance, however, it is often used interchangeably with information assurance (IA). IA is defined in AFDD 2-5 as: “those measures taken to protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality, and non-repudiation.” [18] Given this researcher’s experience in AF network operations, this is a close approximation of the meaning of network assurance; however, the definition should also include attributes of bandwidth utilization and latency, limiting network downtime and increasing network robustness to apply towards the overall network “health” thus defining network assurance. There is also an implied concept of quality of service (QoS) that is sometimes wrapped into the lexicon of network assurance.

Defining mission assurance regarding information technology (IT) assets is not a new concept. Mission assurance was defined back in 2003 in DOD Instruction number 8500.2 and assigned three main categories. The mission assurance category (MAC) “reflects the importance of information relative to the achievement of DOD goals and objectives, particularly the warfighters’ combat mission and are primarily used to determine the requirements for availability and integrity.” [19] The DODs three defined mission assurance categories are:

- The Mission Assurance Category I (MAC I) assets are “systems handling information that is determined to be **vital to the operational readiness** or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of **loss of integrity or availability are unacceptable** and could include the immediate and sustained **loss of mission effectiveness**. MAC I systems require the most stringent protection measures.” [19]
- The Mission Assurance Category II (MAC II) assets are “...**important** to the support of deployed and contingency forces...loss of integrity is unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include **delay or degradation** in providing important support services or commodities that **may seriously impact mission effectiveness or operational readiness**.” [19]
- The Mission Assurance Category III (MAC III) assets are “systems [used] to conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of **loss of integrity or availability can be tolerated or overcome** without significant impacts on mission effectiveness or operational readiness.” [19]

Recently in January 2010, the DoDD 3020.40, mission assurance was defined as a “summation of the activities and measures taken to ensure that required capabilities are available to the DOD to create the synergy required to mobilize, deploy, support, and sustain military operations throughout the continuum of operations.” [20] The commercial and research sectors further peel back the layers of mission assurance beyond the integrity and availability themes of the MACs. In their explanation, mission assurance can also include: system reliability, environmental compatibility, quality assurance, and system safety. Additional attributes of mission assurance included: “materials and processes control, configuration management, risk management and performance verification.” [21] Furthermore, in the new AF Cyber Operations doctrine, mission assurance is defined as measures required to accomplish objectives in a

contested environment through prioritizing functions, mapping dependencies, identifying vulnerabilities and risk mitigation of known vulnerabilities. [17]

Probably the best explanation of mission assurance regarding cyber operations is defined in the *Operating Concept for Hunter Teams (Phase 1)*. There, mission assurance is described as measures needed to achieve essential objectives in contested environments. Failure to provide the means for these objectives significantly impact DOD's ability to perform vital services and/or command and control of forces. [2]

III. Building the Case: Tactical Success Enables Mission Assurance

“Cyber mission assurance is a top priority of the Air Force. . . The domain we are tasked to operate within touches every part of the Air Force and joint mission.” [22]

Maj. Gen. Richard E. Webber
24th Air Force Commander
25 Jan 2010

3.1 Mission Assurance at the Tactical Level

National assets, such as intelligence and communications satellites, previously thought of as just a strategic asset, are also a resource to be employed effectively in tactical operations. [23] Computer networks, especially parts of the GIG, fall into this conundrum. These national forces or assets can be employed for a strategic, operational, or tactical purpose based on their contribution to achieving strategic, operational, or tactical objectives. [23] To understand why mission assurance should begin at the tactical level, the following is a quick review of the three levels of war:

- Strategic level – a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic objectives and guidance and develops and uses national resources to achieve these objectives.
- Operational level – links the tactical employment of forces to national and military strategic objectives through the design and conduct of operations using operational art.
- Tactical level – focuses on planning and executing battles, engagements, and activities to achieve military objectives assigned to tactical units or task forces. [23]

This researcher has spent years in the construction field before becoming a communicator. There are often analogies that can be used from one field to help explain complex problems in other fields. In construction, the most important part

of a project is the foundation. The construction blueprints are the “strategic vision” of the building, and the orchestration of all the activities are akin to the “operational art” to bring it all together. However, without a strong foundation (due to poor materials, poor preparation or poor construction), it does not matter how extravagant and beautiful the house is when complete, because it is only a matter of time before the foundation gives way and at the very least the house realizes some damage if not complete devastation.

Even in a 2005 editorial in the Air and Space Journal, the then deputy chief of staff for Warfighting Integration, Lt Gen Hobbins, while writing on the importance of connectivity, access, and sophisticated information sharing in the field, proclaimed the need to “bring the Global Information Grid down to the tactical edge, fusing our intelligence information to produce real-time situational awareness, thereby enabling effective C2.” [24]

To further illustrate the importance of “winning” from the bottom up, another analogy follows: Imagine a football team of choice, say the Colts, and they are not having a winning season [of course]. They are losing their tactical battles. Therefore, there is no chance then for that team to win the “Super Bowl” and gain strategic victory. Now imagine again, another team, say the Steelers, who are having a winning season and make it to the big game. Although all those small tactical victories do not guarantee a win, those small successes gave the team a chance to gain final victory. Those individual triumphs did provide the **opportunity** to win the strategic goal ... [and they probably will].

Although this last analogy is somewhat light hearted, the point is made. Teamwork and successful execution at the very **tactical** core of the mission enables overall success. In the 2009 Quadrennial Roles and Missions Review Report, it states that the “Department [of Defense] seeks cyberspace capabilities that maintain our freedom of action... while ensuring superiority over potential adversaries.” [25] Furthermore, the

Table 1: Mission Assurance and Network Assurance Relations

| <i>Mission Assurance and Network Assurance Relations</i> | |
|--|-----------------------------------|
| <u>Mission Assurance</u> | <u>Network Assurance</u> |
| Operational focus (A3) | Service provider focus (A6) |
| Assure mission | Assure the network |
| Focuses on operational need | Focuses on service availability |
| Prioritize defense based on critical asset lists | Attempts to defend entire network |
| Proactive based on intelligence preparation | Reactive based on observed enemy |
| Fight through the attack | Disconnect if attacked |

[26]

report stresses the importance of a strong cyberspace capability at all levels [strategic, operational, and tactical] of war to provide:

Friendly “freedom of action...and deny an adversary’s freedom of action... while providing... Global situational awareness [and] warfighting effects within and through the cyberspace domain that are synergistic with effects within other domains.” [25]

3.2 Moving from Network Assurance to Mission Assurance

Freedom of action in cyberspace is a basic requirement for mission assurance. [17]

In a recent (Jun 10) Armed Forces Communications and Electronics Association (AFCEA) Information Challenges Conference, there was a briefing on Challenges to AF Cyber Operations by the 24th AF. On one of the briefing slides was a comparison (although the title of the slide was Mission Assurance vs. Network Assurance, which could be interpreted as a competition against each other) of both mission and network assurance as highlighted in Table 1 on page 14.

The briefing also identified these steps to achieve mission assurance (very similar to the last mission assurance definition in AFDD 3-12): identify the threat, map the network to include the cyber dependencies, map the mission to [the network] architecture through operational planning, and to provide network situation awareness while executing dynamic defenses. [26]

These steps were further expanded. Identifying the threat can mean an internal or external threat, a threat due to a system not yet patched or unable to be patched for one reason or another. Mapping the network (and dependencies) means to know what is connected (with awareness of changes over time), software and processes are running, and performance parameters hardware/software exist. Additionally, mapping the network means to find and close “leaks”, identify critical nodes, dependencies, interrelations, locate single points of failure, ensure all devices are controlled and to enable rapid troubleshooting and re-routing. [26] Finally, to provide mission assurance means applying backups to the failure points transition from passive defensive systems to active ones, build upon a series of progressively secure enclaves through the transition to a strategy based architecture. [26]

The transition from network assurance to mission assurance is not an easy task. The topic was very much at the forefront, in the February, 2011 AFCEA, Rocky Mountain Chapter symposium in Colorado Springs, Colorado. The focus was on “Mission Assurance in Cyber and Space. [27]

The various definitions of network and mission assurance from above are assimilated and boiled down as an attempt to bridge the two terms together. Network Assurance is to protect and defend information and their systems by ensuring: availability, integrity, authenticity, confidentiality, and non-repudiation, necessary bandwidth, limited downtime and increased robustness and quality. In other words... *Be Ready*

Mission assurance is to accomplish objectives through ensuring: systems availability, integrity, reliability, compatibility, quality, safety, processes control, configuration and risk management, and performance verification of information vital to the operational readiness or mission effectiveness of forces in terms of both content and timeliness. Thus... *Get the Job Done*

So when they are tied together, network assurance + mission assurance = *Be Ready to Get the Job Done*.

3.3 *Participation at the Tactical Level: Two Options*

“The way a JFCs organizes their assigned or attached forces directly affects the responsiveness and versatility of joint operations. . . unity of command, centralized planning and direction, and decentralized execution are key considerations.” [23]

There can and will be times to possess and/or execute various CNA/D/E capabilities at the tactical level to ensure mission success. Through the years, the AF communication community has moved from a centralized planning and decentralized execution to centralized planning and execution (via the Integrated Network Operation Security Centers (INOSCs)). The reasons vary from funding, manning, expertise availability, standardization, etc., but regardless, the INOSCs are now positioned to perform the bulk of computer network operations and defensive actions necessary to protect the AF portion of the GIG.

Granted, while the INOSC capabilities focus on more CNO/D efforts, the CNA/E tasks usually fall into the hands of the nation agency partners (US CYBER Command (USCYBERCOM), National Security Agency (NSA)) and other units in the 24th AF (the other military services also have similar capabilities). Ultimately, the geographic combatant commanders (GCCs) will have the final authority over network activities in their AOR during contingencies, but there are options on how to meet this objective [9] because tactical-level operations can be executed by various units and agencies.

There are basically two distinct options or solutions on how to perform cyber operations at the tactical level to ensure mission assurance for the commander. The first option is to rely on external resources such as an INOSC, USCYBERCOM or even NSA to leverage the global reach of the GIG and *tunnel* into the network enclave that needs support. The second option is to have a trained force *on-site* in the AOR that can perform these same actions. Although, the second option involves placing a sophisticated force trained in the art of CNA/D/E, it does have the benefit of proximity for the commander among other advantages. “Decision-making authority

should be decentralized appropriately [and] it should be delegated to those in the best position to make informed, timely decisions.” [23]

AFDD 3-12 relates the tenets of Air Power to Cyber Operations and within that comparison explains centralized control and decentralized execution for cyber operations. This relation, as with the rest of Air Power operations of centralized control and decentralized execution provides the most “effective C2 of capabilities and forces”. The purpose is to provide control by a commander with the strategic view and execution of tasks by those Airmen who best understand the technology and tactical details of a “dynamic operation”. [17]

This researcher recommends the option of placing the **CNA/D/E capability in a Combat Communication Squadron for an on-site cyber force** available to the Joint Force Commander. The following sections, including the research survey statistics and interviews, will further support this option.

IV. Respondent Survey Statistics and Interviews

So far, this research has focused on the communication community’s transition from network assurance to mission assurance to guarantee the deployed commander’s mission success, and recommended doing so, through the option to employ on-site CNA/D/E capabilities at the tactical level. This research will now explore a sampling of the rest of the Air Force that have a vested interest in the future of cyber operations in a contested domain.

4.1 *Survey Overview*

The purpose of the survey was to contribute in the development of evolving cyber operations strategies, thus to further enable deployed capabilities to operate freely in the cyber domain as a part of the JTF Commander to utilize. With the survey sponsorship of Maj Gen Capasso, the SAF/A6O, the survey was approved for distribution. The survey outlined two basic focus areas. They were:

- Current/Recent Deployed Capabilities and Experiences
- Viewpoints on Needed On-site CNA/D/E Capabilities

In coordination with the 689th Combat Communications Wing (689 CCW), the survey was conducted to further explore the roles a combat communications squadron will have in future tactical engagements and help strategic leaders map out new roles for deployable cyber experts.

The survey asked questions related to recent deployable experiences as well as view points on computer network attack, defense and exploitation at the tactical level in an attempt to help shape the Air Force’s future in tactical cyber missions.

The survey, hosted via AFIT’s web sever, was on-line from 1 April to 26 April, 2011 and accessible from either a “.mil”, “.com” or “.edu” computer networks.

4.2 Target Audience

The target audience for the survey were communicators and operators from the A6 and A3 communities throughout the 689 CCW, Air Force Space Command (AFSPC) in the 24th AF including: 688th Information Operations Wing (688 IOW), 67th Network Warfare Wing (67 NWW), 624 Operations Center (624 OC), and other communication (17D) officers throughout the Air Force. It included both officer and enlisted, active duty and some retired personnel but remained completely anonymous.

4.3 Respondent Statistics

With support of this researcher's sponsor, the 689th Combat Communications Wing Commander, Col Giorlando sent a message to the target audience detailed in section 4.2, asking for communicators and operators to complete the research survey. The survey was also sent, out via the Air Education & Training Command (AETC) 17D Functional Manager, to all AETC 17Ds officers. Additional requests were sent to a handful of retired military personnel with similar communication and operational backgrounds.

4.3.1 Statistics Overview. The survey was received with positive results throughout all communities, and in the 26 days the survey was on-line, 211 participants completed it. Job positions were not mandatory in the survey, although of those respondents who identified, included a collection of 38 enlisted technicians, 20 senior enlisted superintendent/flight chiefs, 20 AETC students, 10 crew commanders/OICs, 9 director of operations, 16 flight commanders, 12 squadron commanders, 2 group commanders, 3 wing commanders, a COCOM J6 Brigadier General officer and a retired communicator Major General officer. The rank spread of active duty respondents is presented in Figure 1 on page 20.

4.3.2 Current/Recent Deployed Capabilities and Experiences. The first part of the survey concentrated on deployed experiences of the survey participants in re-

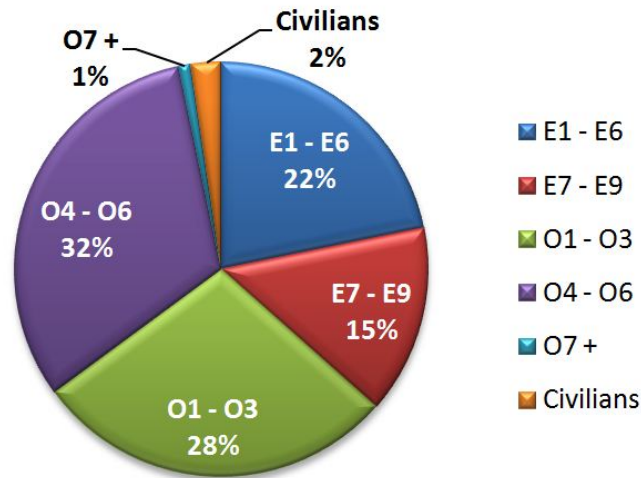


Figure 1: Ranks of All Respondents

gards to supporting the commander with CNA/D/E capabilities. In Figure 2 on page 20, of the 211 respondents, 72 (34%) indicated they had deployed (one or more times) with a tactical communications unit to support a contingency commander. The ranks of the deployed respondents are highlighted in Figure 3 on page 21 with the majority in the officer ranks.

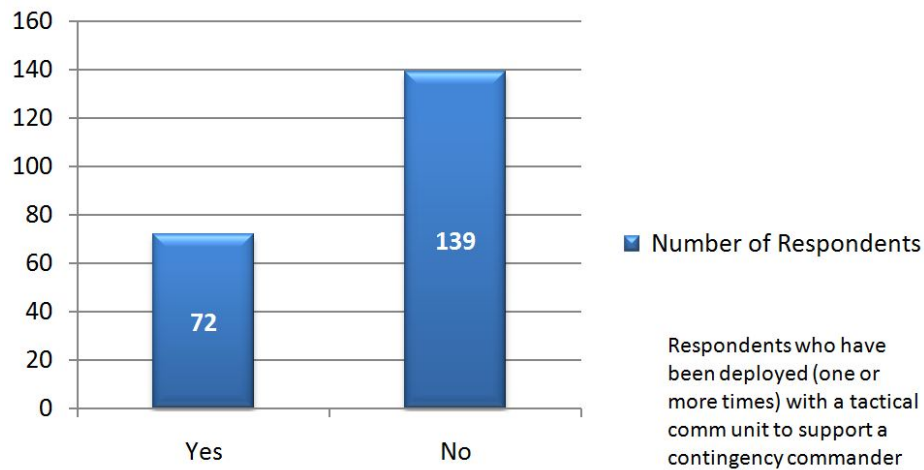


Figure 2: Deployed Respondents

To establish a baseline of the capabilities currently being delivered, the respondents were asked if in any of their deployments did their unit support the commander

in a computer network attack or defense or exploitation capacity. It is not surprising, but the responses were low regarding delivering the CNA/E capabilities for the commander to employ, however the deployed units did perform the computer defense role at about 50% more than the other two as seen in Figure 4 on page 21.

What was surprising though, when asked in any of their deployments did they feel their unit *should have* supported the commander in one or more of the three

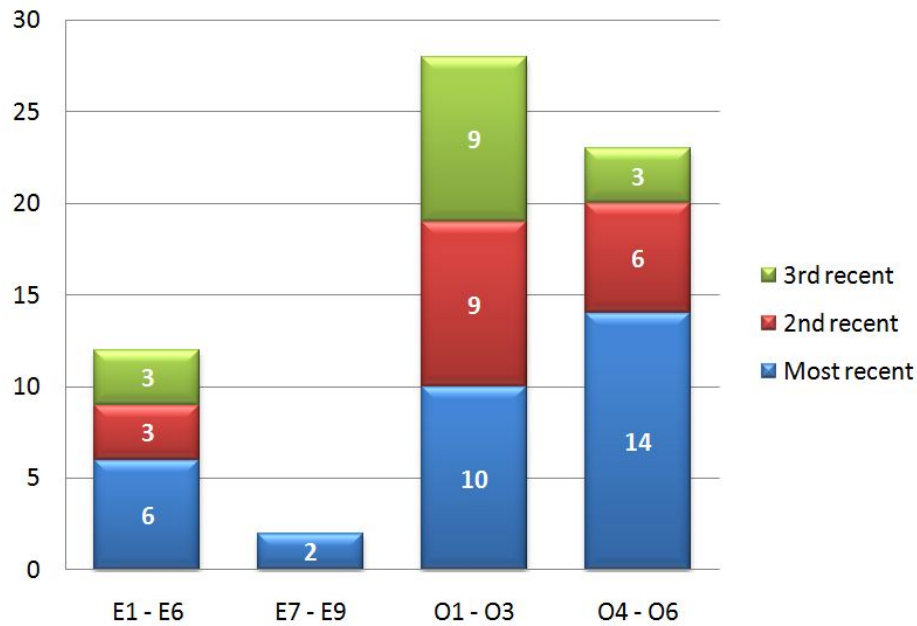


Figure 3: Ranks of Deployed Respondents

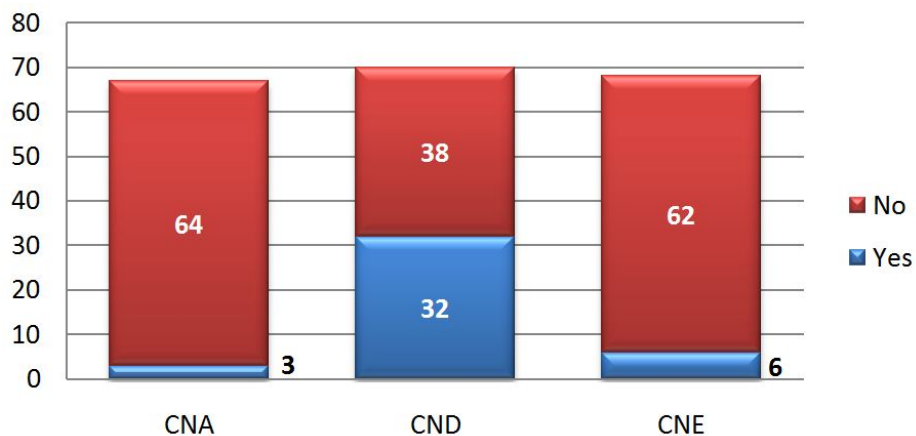


Figure 4: Deployed Unit Supported the Commander in the Following Capacity

capacities, the response for CNA increased nearly four times, CNE more than doubled and CND dropped about 10% as displayed in Figure 5 on page 22.

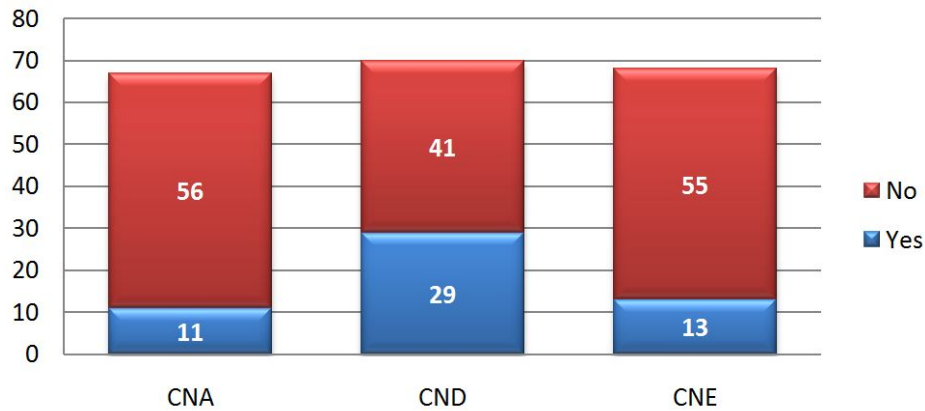


Figure 5: Deployed Unit *Should Have* Supported the Commander in the Following Capacity

4.3.2.1 Barriers to Deployed CNA/D/E Capabilities. There must of been reasons why these deployed Airmen did not perform these cyber tasks. To get to the heart of why they did not, those who indicated they feel their unit *should have* supported the commander in one or more of the three cyber tasks during their deployment, the respondents were further asked to identify potential barriers and rank their importance. The barriers available for selection were **Policy/Rules of Engagement (ROE)**, **Legal**, **Lack of training** in one or more of the CNA/D/E fields and **Other**.

These barriers were derived from various class lectures and readings while here at the Air Force Institute of Technology (AFIT), listening to various Air Force leaders over the years and from this researcher's own experiences in the field of common hurdles to overcome while accomplishing the mission at hand. These barriers and additional rationale are used and will be discussed later so that a common baseline of solutions can be developed to mitigate these barriers. As seen in Figure 6 on page 23, these barriers are highlighted and ranked. Taking into account the **Important** and **Very Important** rankings, both barriers of **Policy/ROE** and **Lack of training**

were identified as the majority of the issues with almost double the votes of the other two barriers. This trend is seen as a common theme later in this research.

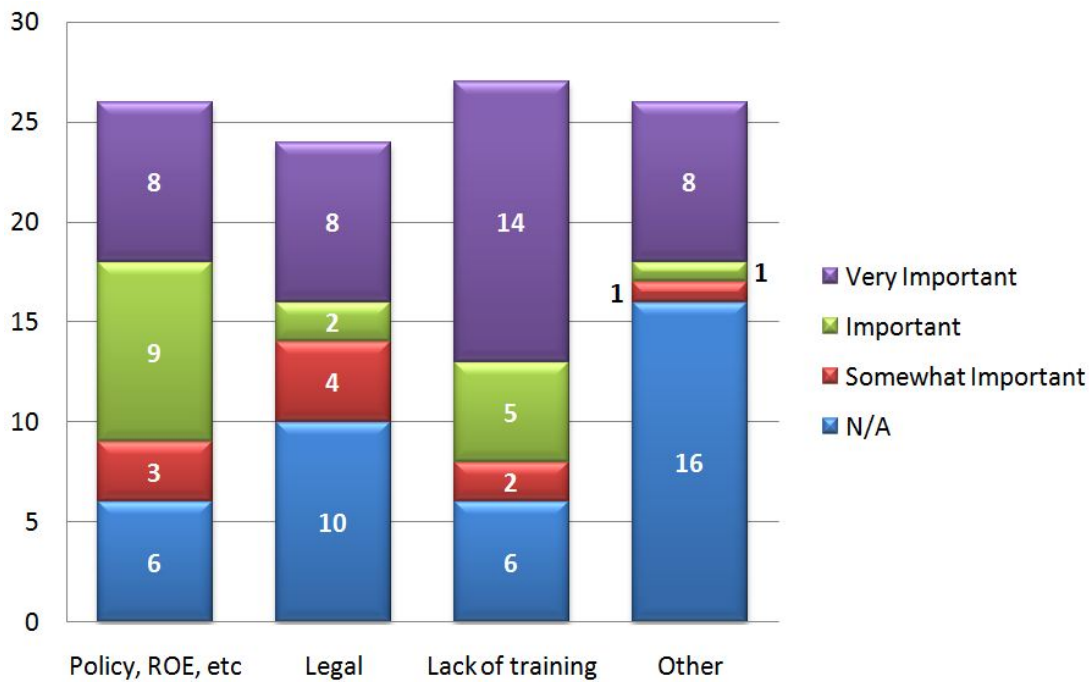


Figure 6: Barriers Why Unit *Did Not* Support Commander While Deployed

Finally, the deployed respondents were asked to their knowledge, did any other unit support the commander in any of the CNA/D/E actions. Only seven (10%) of the deployed respondents indicated they knew of other units that did perform some part of computer network attack, defense and/or exploitation, but could not be specific due to classification levels

4.3.3 Viewpoints on Needed On-site CNA/D/E Capabilities. Moving from actual deployed examples, the second part of the survey was divided into two groups of respondents. One group believed it is necessary for the supported commander to have the option to employ any of the CNA/D/E actions at the tactical level by a deployed tactical unit. The other group did not. Figure 7 on page 24, displays whether or not each respondent believes this cyber capability should be utilized on-site tactically.

Section 4.3.3.1 will focus on those respondents that *did not* believe it necessary to employ on-site tactical computer network attack, defense and/or exploitation.

4.3.3.1 Against – Needed On-site CNA/D/E Capabilities. The 69 respondents (33%) who did not foresee the deployed commander tasking one of their local units to execute a computer network attack, defense and/or exploitation task against the advisory were asked their rationale by selecting one or more reasons and ranking their importance. Similar to the barriers identified in section 4.3.2.1, these barriers, now referred to as the *rationale against* this deployed capability were: **Policy/Rules of Engagement (ROE)**, **Legal**, **Lack of training** in one or more of the CNA/D/E fields and **Other**, but also included the options of already **happens remotely** from other units and/or **Not an on-site unit’s mission**. In Figure 8 on page 25, taking into account *important* and *very important* rankings, 70% of those respondents indicated that these CNA/D/E functions already *happen remotely* and it is equally split at 54% for *not an on-site mission* and *lack of training*. *Policy/ROE restrictions* and *legal concerns* make up 35% and 29% respectively.

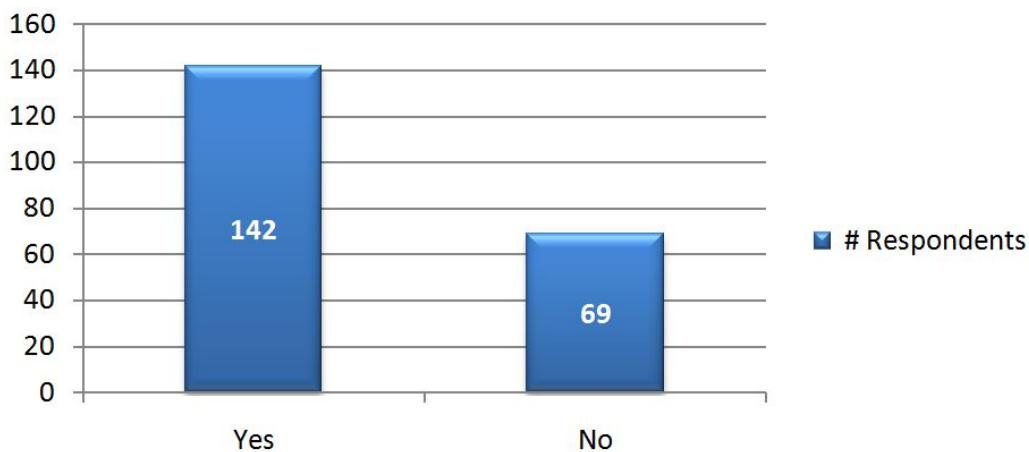


Figure 7: Deployed Commander *Should have* an On-site Tactical CNA/D/E Capability

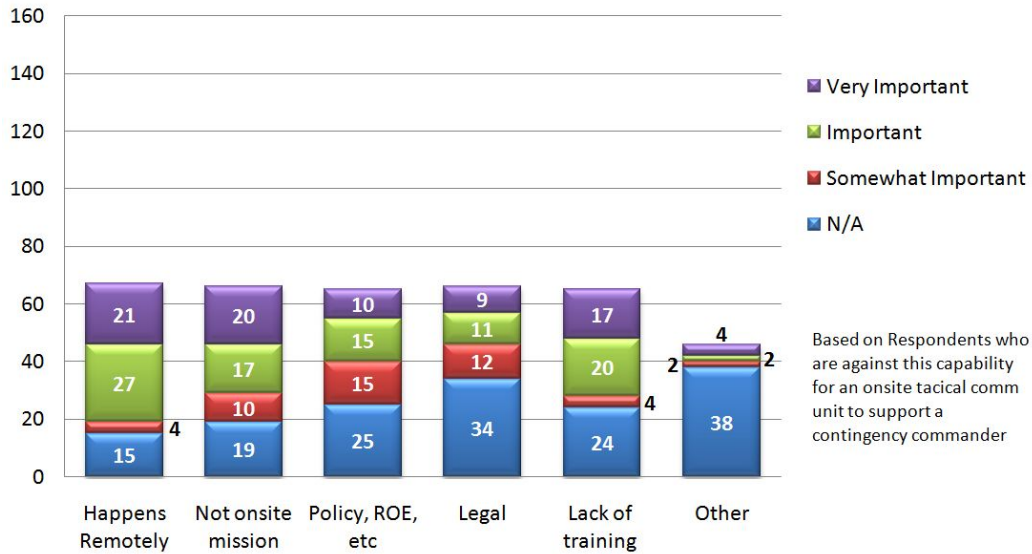


Figure 8: Rationale *Against* an On-site Tactical CNA/D/E Capability

The ranks of these active duty respondents are closely distributed, with 58% officers and 42% enlisted Airmen. Figure 9 on page 26, shows the breakout with field grade officers having the majority vote against the capability. There were also two respondents retired from the military, one was a field grade officer and the other a senior enlisted Airmen. Common themes (three or more occurrences) for their rationale included (in order of frequency):

- Only CND should be a tactical units responsibility
- Skill-sets require focused knowledge
- CNA/E is predominately a Strategic function (not tactical)
- Possible dilution of expertise (“Jack of all trades”) by tactical unit
- CNA/D/E should be centralized for unity of effort (otherwise duplication of efforts possible)
- CNE is predominately a Title 50 function, not to be done by Title 10 forces
- Policy/ROE needs amendments/revisions

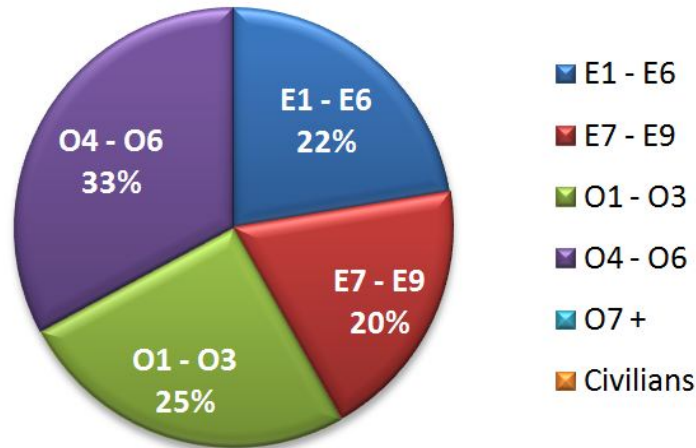


Figure 9: Active Duty Ranks of Military Respondents *Against* an On-site Tactical CNA/D/E Capability

An interesting statistic by grouping the ranks by their “most likely age”, the younger (E1-E6 and O1-O3) and older (E7-E9 and O4-O7+ and civilians) populations were almost evenly split as seen in Figure 10 on page 26, with the “Older” population in the slight lead.

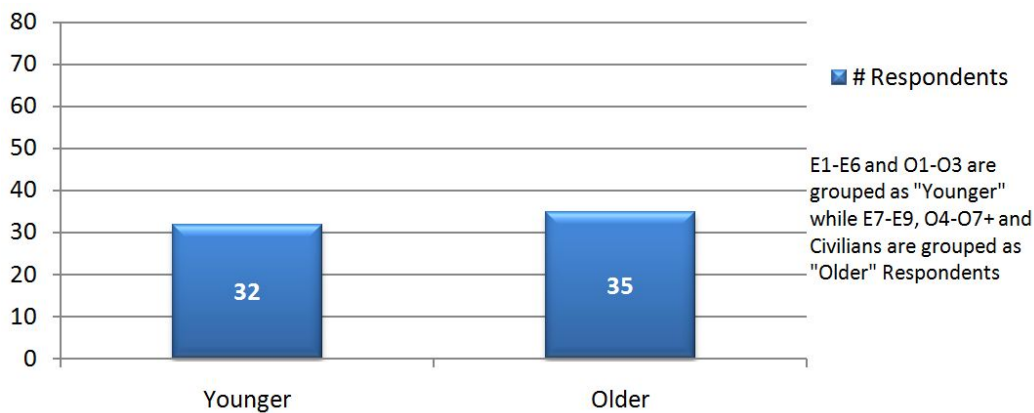


Figure 10: Active Duty Respondents *Against* an On-site Tactical CNA/D/E Capability

Section 4.3.3.2 will focus on those respondents that *did* believe it necessary to employ on-site tactical computer network attack, defense and/or exploitation.

4.3.3.2 *For – Needed On-site CNA/D/E Capabilities.* The 142 respondents (67%) who feel it is necessary for the supported commander to have the option to employ any of the CNA/D/E actions at the tactical level by a deployed tactical unit were also asked their rationale by selecting one or more reasons and rank their importance. Identical to the barriers identified in section 4.3.2.1, these reasons, again referred to as barriers to this deployed capability were: **Policy/Rules of Engagement (ROE), Legal, Lack of training** in one or more of the CNA/D/E fields and **Other**.

In Figure 11 on page 27, taking into account *important* and *very important* rankings, 81% of those respondents indicated that *Policy/ROE restrictions* are of top concern followed closely by *Lack of training* at 73%. Legal concerns make up 56% of the votes.

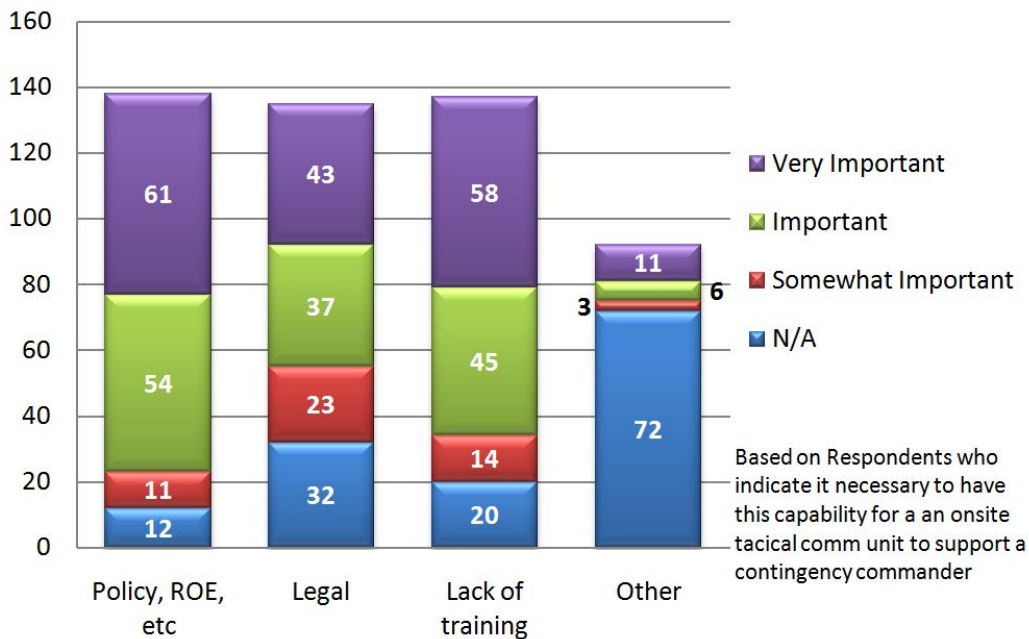


Figure 11: Barriers to an On-site Tactical CNA/D/E Capability

The ranks of these active duty respondents are distributed with 64% of officers and 33% being enlisted Airmen and 3% being government civilians. There were also nine respondents retired from the military, three were field grade officers, one

General officer, four were senior enlisted Airmen and one retired civilian. Figure 12 and Figure 13 on page 28 show detailed rank break out for Active Duty and Retired respondents respectively.

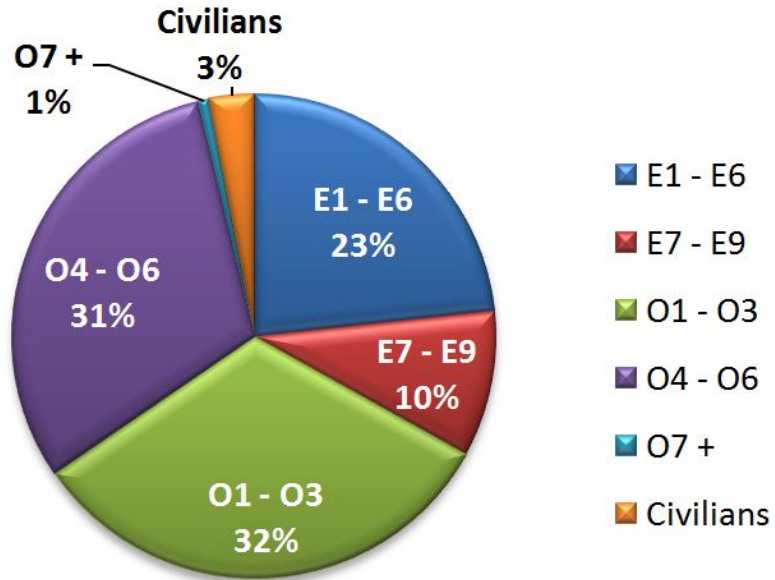


Figure 12: Active Duty Ranks of Military Respondents *For* an On-site Tactical CNA/D/E Capability

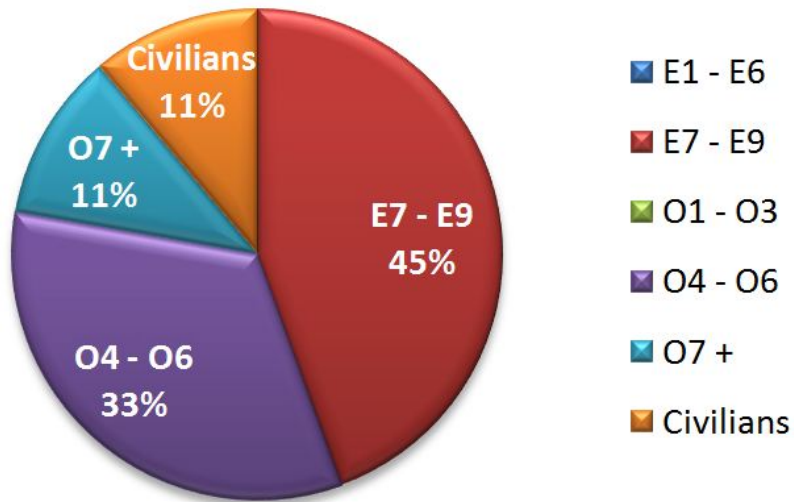


Figure 13: Retired Ranks of Military Respondents *For* an On-site Tactical CNA/D/E Capability

Common themes (three or more occurrences) for their barriers included (in order of frequency):

- Commanders do not understand cyber capabilities, therefore do not employ them
- Blurred/burdensome/conflicting C2 structures
- Speed of approval of actions (red tape)
- National level policies not flexible
- Confusion of appropriate legal CNA/E actions
- Second/third-level effects (collateral damage)
- AF-level policies still in flux
- Lacking skill-set/capability (CNA/E) in deployed units
- Training programs outdated/do not change quick enough to keep up with technology/techniques
- Title 10/50 Conflicts
- CND at tactical units (not CNA/E)
- Tools not same at tactical networks or non-existent
- Access to employ tools at tactical level
- Retention issues for trained force

Keeping in line with section 4.3.3.1 the ranks were grouped by their “most likely age”. The populations as seen in Figure 14 on page 30, show the “younger” population in the lead at 56%, versus the “older” population at 44%. This could be explained as the younger respondents being more receptive to the technologies needed for this capability, or just a larger population polled, none-the-less, it is an interesting statistic.

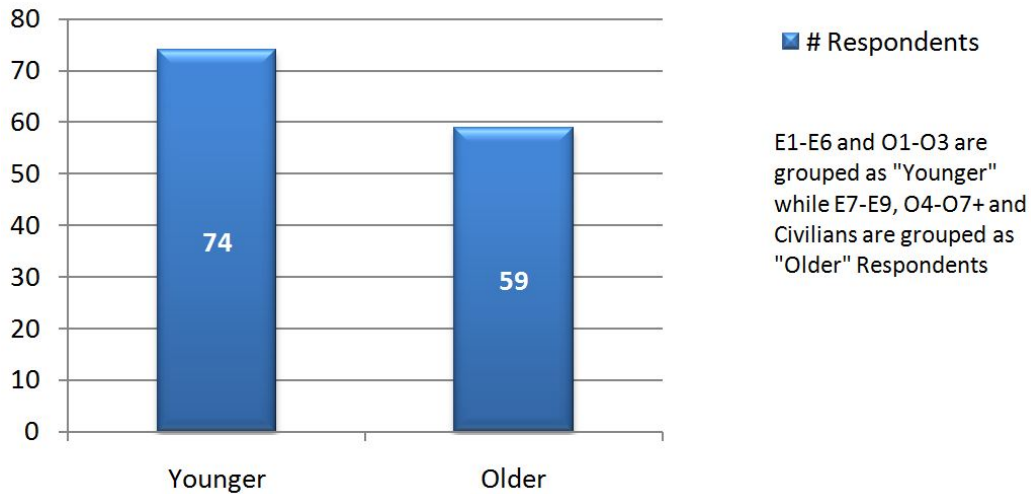


Figure 14: Active Duty Respondents *For* an On-site Tactical CNA/D/E Capability

4.3.3.3 Communicators and Operators Comparison. To prove that the survey was not biased towards the communication community, the respondents were asked what their primary experience consisted of, either in the A6 (communications) or A3 (operations) community. Figure 15 on page 30, displays the complete breakout between A3 and A6.

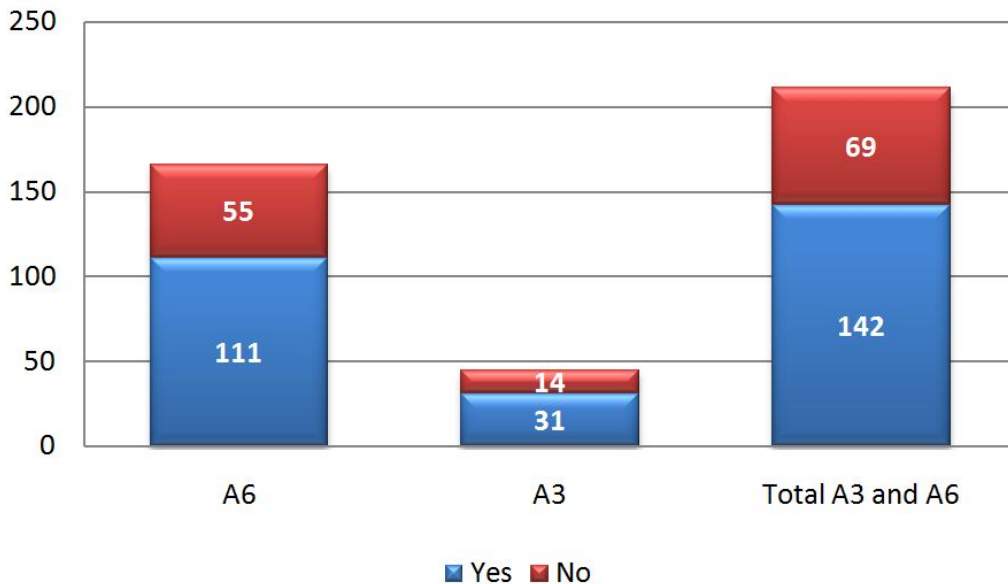


Figure 15: Total Respondents who believe it *IS* or *IS NOT* necessary to have an On-site Tactical CNA/D/E Capability

To put the communities in perspective of their populations surveyed, Figure 16 on page 31, displays how each community believes these cyber capabilities should be available to the deployed commander and interestingly, the A3 community had a higher percentage of “Yes” votes than the A6 Airmen.

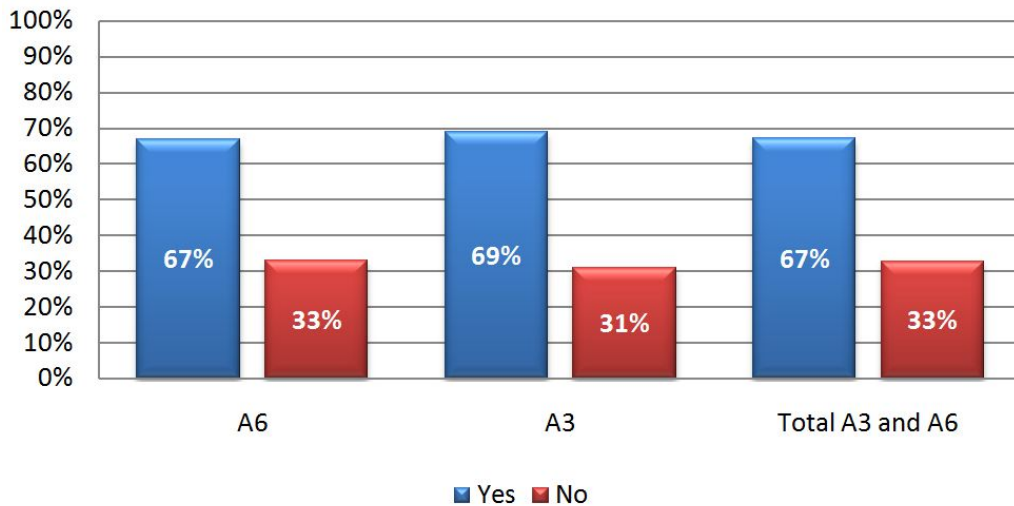


Figure 16: Percent of Responses who believe it *IS or IS NOT* necessary to have an On-site Tactical CNA/D/E Capability

Finally, to show the percentage of how all the respondents voted by their communities in relation to needing CNA/D/E at the deployed tactical level, Figure 17 on page 31 showcases this relationship.

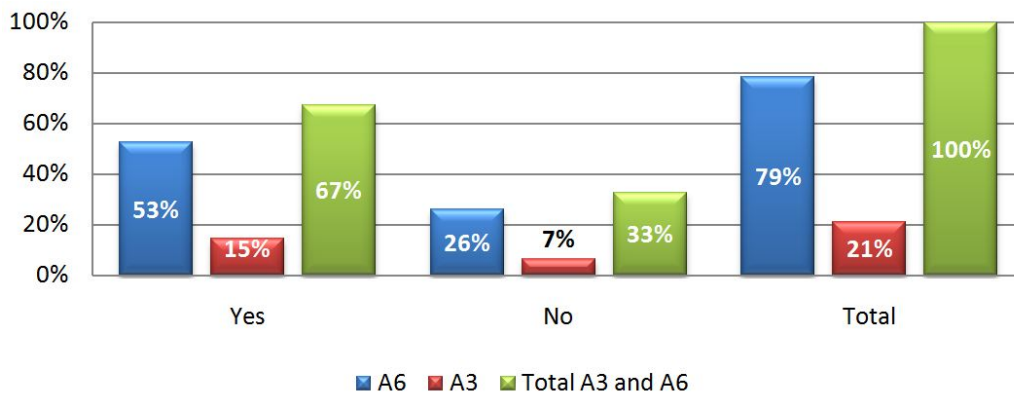


Figure 17: Percent of Respondents who believe it *IS or IS NOT* necessary to have an On-site Tactical CNA/D/E Capability

The overall statistics combining both the A3 and A6 responses for “Yes” or “No” in Figure 16, show an overwhelming 67% of the respondents that computer network attack, defense and exploitation at the tactical level *should be* available to be employed by a JTF commander

4.4 Interviews

This researcher also had the honor to interview four innovative strategic leaders on the cutting edge of cyber operations. The following sections highlight the thoughts, insights and experiences of these leaders related to this research. This researcher has received the approval from all four interviewees to include the following excerpts of their interview conducted. Approval “letters/emails” from the interviewees are included in Appendix A.

The interviewees were (in no order of military rank):

- Air Force Special Operations (AFSOC) A6, Col Von Gardiner
- US Transportation Command (USTRANSCOM) J6, Brig Gen Earl Matthews
- 688th Information Operations Warfare (IOW) Commander, Col Robert Skinner
- 689th Combat Communications Wing (CCW) Commander, Col Theresa Giorlando

The following four sections highlight key points and recommendations of these cyber leaders.

4.4.1 Air Force Special Operations (AFSOC) A6 . Col Gardiner was deployed as the J6 for US Forces during Afghanistan operations under the command of General McChrystal. Col Gardiner had visibility over all US (Joint Operational Area) JOA networks (including all Army, Navy Air Force, Marine Corps nets) that traversed that AOR. This presented problems due to “owners” wanting to control their portions of the network. For example, Air Force Central Command (AFCENT)

wanted to control everything down to the desktop and Joint Special Operations Command (JSOC) wanted control of “their assets” as did the specific services. To control the chaos, a Joint Network Control Center (JNCC) was established to perform oversight on configuration management and control and network management for all US forces in theater to direct compliance of user networks and ensure interoperability in the AOR.

This JNCC lacked the reach back to partners (such as NSA) and did not have the expertise or tool sets available for the staff in the JNCC that one, “knew the network” and two, were able to investigate the joint network to “hunt out” network anomalies that were not necessarily malicious, but questionable. Some of these “questionable” activities included large file movements that did not make sense for a specific users profile (i.e. they were not a system manager).

To address this challenge, Col Gardiner first stood-up a “green team”, aka, a “find and fix” team to visit major operating locations and sit alongside the JNCC technicians. Their immediate charter was to get a handle on the network management and configuration of the joint network. This green team ran the tools necessary to identify these anomalies, help the technicians fix the issues, document the findings and provide training to the JNCC and local network personnel. The green team consisted of a handful (six) of experts from the NSA, Joint Task Force-Global Network Operations (JTF-GNO) and the services, all pulled together by US Central Command (USCENTCOM).

Second, Col Gardiner created a “hunter team,” formed from personnel from NSA and JTF-GNO through agreements, handshakes and meetings with leadership to make it happen. The hunter team sat alongside the JNCC service members, contract personnel, etc. all fully integrated into the team of the JNCC. Where this hunter team made the greatest impact was their ability to interact with NSA back in garrison and be a sounding board between the National Security Agency (NSA)/Central Security Service (CSS) Threat Operations Center (NTOC), and the JNCC. Therefore, when

global network change orders were issued that would possibly “break” the network in theater, the hunter team, armed with the proper understanding of “why it would break it” due to their intimate knowledge of the network architecture could advise leadership of potential impacts and optional mitigating actions.

Additionally, this hunter team with the tools [from back home] was able to compare findings with their counterparts at NSA and JTF-GNO and the local deployed operation centers to identify possible threats and decide holistically [and Nationally if needed], the correct course of action (COA) to deal with this “threat.” This avoids the tendency of “reach back” support to just “disconnect” the threat without understanding the mission assurance impacts of degraded service during combat operations. Therefore, the hunter team was successful because they had the right situational awareness of operations in theater to choose the correct COA, because of their proximity, embedded nature and team building with the JNCC.

Col Gardiner also recommended the need for continual training on the necessary tool sets already in use in garrison and agreements between those technicians and the experts at NSA and USCYBERCOM. So, when the time is at hand for deployment, the personnel are proficient with the tools and [command and working] relationships are already established. Just-in-time training and ad hoc partnerships are *not* the answer to remain proactive in a contested cyber environment.

Furthermore, Col Gardiner agreed to this researchers recommendation of development and use of “cyber munitions” at the tactical level with the caveat and caution of second and third order effects. It is the collateral damage that must be considered in all levels of conflict across the range of military, political, and economic implications. The reusability of the cyber munitions is also a consideration prior to employment due to the extensive research and “one-time” use of most of the tools.

Finally, he stressed the importance of proper coordination and recommended a “true fused operations center to include representatives from all disciplines [intel, cyber, traditional weapons systems] during all phases of the campaign to provide the

commander a complete set of COAs and risk assessments both offensive and defensive to eliminate, or at least minimize potential fratricide.”

4.4.2 US Transportation Command (USTRANSCOM) J6. General Matthews foot stomped the need that tactical level communicators *must* have adequate CND capabilities. The general noted that most CND actions provide intelligence due to their nature of watching network traffic and actions. This “intel” should be centrally reported and analyzed. There are not yet the legal authorities for “right of self defense on the network, but they will come”. This is due to the consequences of second and third order effects in the cyber domain that cannot be explained with certainty or quantify their cascading effects. Additionally, US policy still considers Cyber as a strategic weapon, so the authorities for cyber actions must originate from POTUS.

Furthermore, due to the global nature of US forces, opportunities are opened for the deployed units to employ CNE efforts and send the findings forward to the intelligence communities. The combined CND and CNE intelligence gathered under the JTF commander provides a powerful assessment and awareness of the networks. This success [realized] at USTRANSCOM is due to the collaborations between the J2 and J6 for the synergistic effects of combined cyber operations and intelligence.

Finally, General Matthews stated the “components that support the COCOMS [24th AF and in turn the combat communication squadrons being one of them] should actually execute cyber operations and are good candidates to perform CND [and possibly CNA/E] actions necessary under USCYBERCOM.” He reinforced that CNE must proceed any offense [CNA] action to pinpoint the target and limit [collateral] effects; and [when asked] he agreed to the employment of “cyber munitions” similar to the complexity and precision of the Stuxnet worm during military operations.

4.4.3 688th Information Operations Wing (IOW) Commander. Col Skinner agrees “there should be an expeditionary CNA/CNE full spectrum capability ... to include CND at the tactical edge”. Policy issues include the differing opinions of the

JTF Commander (JTF/CC) and USCYBERCOM regarding: where the demarcation of the [JTF/CC's] network begins/ends, who controls what assets and when these network assets are deployed ensuring the right coordination occurs in a synchronizing of fires. Possible solutions include network “corridors” that the JTF/CC could operate within while coordinating activities between the national agency partners and USCYBERCOM and at the same time keep the balance of authorities in relation to the operations being performed.

Initially, there might not be enough capacity in a CCS or expeditionary unit full time due to manning and expertise levels. The full spectrum operator [who performs these CNA/D/E activities on a daily basis] might not need to be ingrained in a CCS, but could just augment the CCS during an expeditionary mission, at least initially. This augmentation Unit Type Code (UTC, explained in section 5.1.3) should be an assigned UTC in a sister unit in the 24 AF, not resident in a CCS.

In a similar reflection Col Gardiner mentioned, Col Skinner also believes the relationships between the cyber operators should already be established and exercised on a continual basis, not just before a deployment tasking. However, it makes more sense for a CNA/E team to be assimilated into the CCS at time of need instead of a CCS integrating itself when ready to deploy forward because these relationships are already established in CCW's sister wings [67 NWW and 688 IOW]. Col Skinner went on to say, this does not mean that in the future these relationships between the CCW and their sister wings will not become established to allow the UTC to reside in a CCS, but it will take time and a culture change to make a reality.

Col Skinner is directly involved in more formal “Hunter teams” mentioned earlier in Col Gardiner's experience. These hunter teams are rapid reaction teams that deploy through deliberate or crisis action planning scenarios that deploy physically or virtually to “hunt out the adversary on the network”. The hunter teams follow legal rules that allow them to scout the AF network and at times, [given proper legal authorities] traverse outside the AF network and look for warning and indicators of

an “active persistent threat”. The hunter teams have [since interview (in April 2011)] deployed in a team of four to six personnel with skill sets tailored to the mission using existing 92 IOS tools and capabilities to place “physical sensors throughout the network to monitor the threats.”

The second mission set of the hunter teams under Col Skinner’s command focuses on providing mission assurance on particular segments of networks that prepare the network [battle space] prior to that mission activation on the required network segment. They inspect critical links and nodes to ensure there are no external threats that would degrade the ability to execute the mission initially and provide continued defense throughout mission completion if required.

Currently, these hunter teams fall under control of the 624th Operations Center (624 OC) and have only been tasked to support in garrison internal AF bases. The 624 OC coordinates all legal authorities needed to examine the AF or extended networks. Typically, the first type of hunter teams are tasked directly by the 624 OC to engage their skills to keep vigilance on portions of the AF network and the mission assurance hunter teams are requested by the A3 of the owning mission set to be supported. At the time of this research there have been approximately ten activations of the combined hunter teams in the past 18 months.

4.4.4 689th Combat Communications Wing (CCW) Commander. Col Giorlando outlined three “visionary priorities/themes” of where the CCSs need to evolve in the future. They are:

- Integrating the capabilities of the three 24 AF Wings
- Ensure the traditional CCS mission does not lose their core capabilities
- “One-Off Scenario”

4.4.4.1 Integrating the capabilities of the three 24 AF wings. This integration leverages the synergy of the three wings. Possible synergistic efforts might

include embedded Hunter Teams with a deployed CCS. Additional efforts include coordinating bare base network design with 38th Cyberspace Engineering Group (38 EIG) prior to a network deployment to make the transition to permanent network sustainment smoother and use the CCS to augment the task to expand the AF Network into a one “.af.mil” network. This theme is in step with the focus of this research for the need of traditional CCS to expand their capability to include computer network attack, computer network defense and computer network exploitation functions.

4.4.4.2 Ensure the traditional CCS mission does not lose their core capabilities. The CCSs have a long legacy of traditional combat communications including bare base air traffic control and communication network capabilities. The AF has recently shifted the mission sets of nine traditional Air National Guard (ANG) CCSs to the new cyber focus to grow this new AF capability. This move now puts the balance between active duty and ANG units at 50-50 where the ANG units used to have the preponderance of the CCS traditional capability. Care must be taken not to transition too far and cut too deep as to lose the traditional bare base mission set capability for the COCOMS.

4.4.4.3 “One-Off Scenario” . Col Giorlando described the need for a homogeneous AF network through to the tactical edge. Currently this is not possible [due to different configurations and equipment utilized]. The 24 AF cannot “see” into the deployed networks to monitor the network at the tactical edge. However, as these networks continue in their interoperability merger, there is a potential for common vulnerabilities and exploits between the fixed base and tactical base networks.

For example, if the CCSs are tasked to support an in garrison base that was subjected to a computer attack and the CCS network configurations were identical to that of the crippled base, the CCS’s network will also be subject to the same vulnerability and adversary exploit. Therefore, the tactical networks should be designed a bit different than in garrison base networks to avoid potential complete outages. But most importantly, these design changes should be deliberate and consistent across

the CCSs to allow the greatest interoperability and least compounded vulnerability scenario possible. This slight design difference between the in garrison networks and the deployed networks is the “One-Off Scenario”.

V. Survey and Interview Analysis and Recommendations

5.1 *Preparing a Combat Communication Squadron for this New Mission*

The preceding survey statistics highlighted in section 4.3.3.2, with 67% of the respondents who believe it is necessary for the supported commander to have the option to employ any of the CNA/D/E actions at the tactical level by a deployed tactical unit, indicate the focus of this research is spot on.

The following sections will concentrate on over coming some of the barriers previously noted and recommend how to phase in this capability into the CCS mission set to provide the full spectrum of cyber operations from the forward location via decentralization execution, not through centralized remote access.

- Policy and Legal Concerns
- Training Concerns
- Current Structure
- Proposed Structure
- Proposed Tool Sets
- Time Phased Implementation

The end of this chapter suggests some final thoughts of on-site tactical CNA/D/E and recommendations to overcome some of the challenges mentioned in this research.

5.1.1 Policy and Legal Concerns. Section 2.3 outlines the NMS focus on “joint assured access to the global commons and cyberspace constitutes a core aspect of U.S. national security and remains an enduring mission for the Joint Force.” [10]

In the event of a broad reaching attack by state or non-state actors, the US must have various achievable and implementable options to fight through these attacks and hold those adversaries accountable. To do this, “we [the United States] must seek executive and Congressional action to provide new authorities to enable

effective action in cyberspace.” [10] The policies currently active, mandate the need for continued involvement to ensure the necessary legal authorities are in place to conduct the full range of cyber operations. The 24 AF, as the Air Force’s lead in the complete spectrum of cyber operations on the AFNet, has through their 624th Operations Center (624 OC), concentrated all authorities in the USC necessary to perform all cyber operations. Figure 18, on page 41, details the USC authorities within the 24 AF.

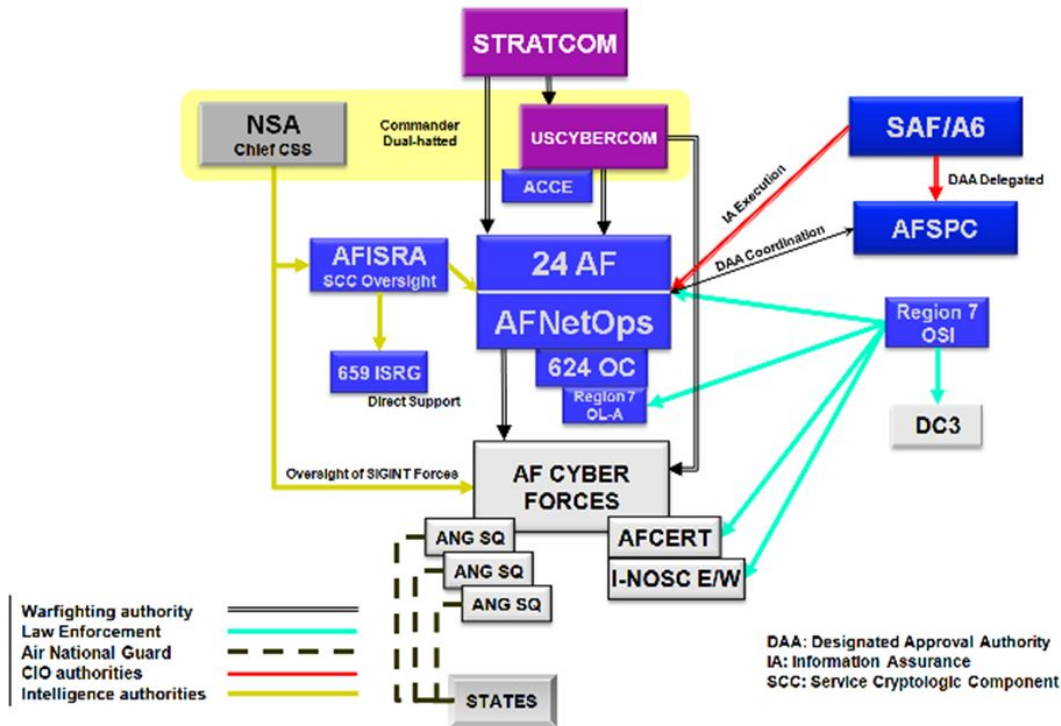


Figure 18: United States Code Legal Authorities within 24 AF [1]

These same agreements must also be in place in the JTF/CC’s AOR to direct and coordinate legal authorities during JTF contingency operations.

5.1.2 Training Concerns. Air Education and Training Command (AETC) has developed various cyberspace specific curriculum for officers, enlisted and civilian personnel. The core set of training for cyber (17D Air Force Specialty Code (AFSC)) officer accessions is the new Undergraduate Cyber Training (UCT). UCT will consist

of content from the previous Communication and Information (C&I) Basic Communications Officer Training, C&I Officer Network Training, 8570.1M (Security +), and Undergraduate Network Warfare Training (UNWT). The training will include information to design, secure, assess, exploit, attack, and defend seven types of networks: Telephony, Internet Protocol, Satellite, Land Mobile Radio, Industrial Control Systems, Integrated Air Defense, and Tactical Data Link. [28] There is projected to be 115 training days per class with an annual throughput of 493 17D's scheduled per year. As of Feb 2011, there has only been 6 of these students assigned to a combat communication squadron.

Additionally, AETC has revamped their enlisted cyber training programs as well. Their enlisted (1B4 AFSC) program will provide initial skills training to supply "Cyberspace Defense Operators" to various cyber operations units across the Air Force. Much of the 1B4 training is identical to the 17D officer training in order to have the same knowledge level before they begin the second stage of training, the Intermediate Network Warfare Training (INWT). These Cyberspace Defensive Operators are trained in "operating the network and computer-based detection and deception systems; performing technical analysis of networks used by warfighters and agency partners to determine effective defensive maneuvers in case of attack." [29] There are classes planned for every six weeks with up to 12 students each. That equates to approximately 70 students per year, given the current schedule. [29]

The follow-on INWT training, hosted by the 39th Information Operations Squadron (39 IOS), is an intensive 42 day course to include education in policy, doctrine, employment, [other cyber] executing organizations and missions, operational functions, and law and ethics. The cyber students study several critical areas including "mission employment and coordination of network attack, network defense and network-warfare support activities." [30] The 39 IOS anticipates a student throughput at "eight INWT courses per year with an average of 24 students each". [30] That equates to 192 students per year. Statistics were not available for those enlisted students graduating

the Cyberspace Defensive Operation or INWT courses with assignments to a combat communication squadron.

Finally, AETC has two programs at the Air Force Institute of Technology (AFIT) focused on cyber operations. The first is an 18 month graduate program geared towards company grade officers, senior enlisted and civilian students in a “Cyber Operations” Graduate (GCO) program. The program curricula involves areas of: “CNA/D/E cryptography, computer forensic, systems security engineering and operations, application software security, and threat and vulnerability assessments/-analyses. Cyber Operations also encompasses managerial aspects such as: strategic and tactical planning for INFOSEC, managerial and engineering ethics, legalities, managerial roles and responsibilities, risk management, information assurance systems, and product acquisition.” [31] The GCO class size range between 20 and 30 students per session.

The second AFIT program is available to officers in the grade of Major (O4) in any of the military services to include civilians of similar “rank”. This 12 month accelerated program is the Intermediate Developmental Education (IDE) Cyber Warfare program designed to provide students a “broad background in cyber warfare theory and application, thereby providing graduates with a foundation to better understand, develop, acquire, manage and employ cyber-based capabilities now and in the future. Students are then educated in cyber war applications, to include network defense, attack and exploitation.” [32] The IDE program, over the past two years (2010 and 2011) has graduated 5 and 12 students respectively, and will have 7 students in the next (2012) class. This last student decline raises some concern in the focus the Air Force desires its operational and strategic cyber leaders to obtain. One would think the class size would increase or at a minimum maintain the current capacity. To this researcher’s knowledge, neither of the two AFIT programs have sent a graduate to a combat communication squadron as an immediate follow-on assignment.

All of these AETC programs collectively encompass training to prepare the tactical expert to the strategic leader and are a solid foundation to the Air Force’s committed effort to bolster its Cyber Warfare capability. What seems to be lacking is the same commitment to place graduated students into the combat communication units. This in-balance needs to change to afford the capabilities in lacking CNA/D/E expertise for deployed communications.

5.1.3 Current Structure. A UTC (Unit Type Code) is the basic building block of all Air Force units and is organized as a predefined standardized grouping of manpower and/or equipment to provide a specific wartime capability. The basic UTCs in the CCSs begin with a “6K” that means Communication and Information systems. The basic capability of all CCSs provide complete activation of voice and data [unclassified and classified networks] services to support the warfighter in contingencies at expeditionary airbases or bare-base locations world-wide. These 6K UTCs include everything from power generators to small arms for perimeter base protection and complete communication capabilities including email, print services and file servers and can build upon the initial UTC to provide increasing numbers of warfighter personnel. [33]

The current 24th AF structure in Figure 19, on page 45, displays the CCSs as a part of the Combat Communication Wing (CCW) under one of the two Combat Communication Groups (CCG).

5.1.4 Proposed Structure. Change often occurs through observations and learning in the surrounding environment. The operational environment in the cyber domain is constantly changing to meet the needs of the warfighter. The following sections attempt to address a new UTC structure through learning from other similar units (Hunter Teams).

5.1.4.1 Hunter Teams . Military operations, especially sustained commitments of the US forces, often breed “out-of-the-box” thinking and creative/inno-

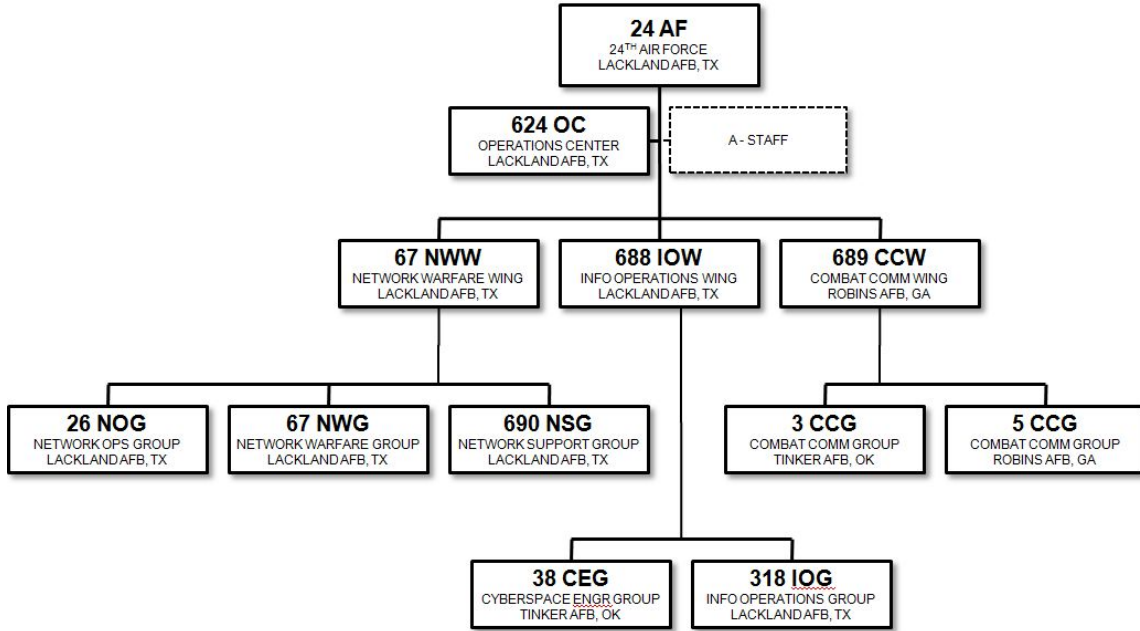


Figure 19: 24th Air Force Structure [1]

vative solutions arise from the experiences of the military personnel currently engaged in “the fight”. The interview, in section 4.4.1, of Col Gardiner’s experiences in Afghanistan with his “Hunter Teams” is no exception. Since then, the 24 AF has implemented a formal Hunter Team concept detailed in the *Operating Concept for Hunter Teams (Phase 1)*. [2]

This Hunter team is currently organized under the 688th Information Operations Wing (688 IOW) out of an initial cadre of personnel from the active duty 92nd Information Operations Squadron (92 IOS) and the Air National Guard’s 262nd Network Warfare Squadron (262 NWS). [2] The 262 NWS is one of the ANG units referred to in section 4.4.4.2 that has been re-tasked to grow the new cyber mission focus of the Air Force. These two units are tasked to “build training plans, gather requirements and establish standard operating procedures (SOPs).” [2]

Currently, the plan [most likely due to manning and funding short-falls] only calls for *three* Hunter teams established through fiscal year (FY) 2012. The “out-the-door” team composition calls for six personnel to perform 24/7 operations at a single location. However, the duration of the team mission tasking is only to last

for a few weeks. [2]. This could become problematic in reacting to active persistent threats where continual CND actions are needed to repel adversary attempts to access warfighting networks.

The current Hunter team mission is provide “mission assurance at key network links/nodes *within the AFNet* on AF or Joint Base installations”. [2] At least through FY12, there does not seem to be a capability to assist the Joint Warfighter outside the AFNET at contingency locations world-wide.

5.1.4.2 Hunter Team Composition . The 688 IOW Hunter team composition is displayed in Figure 20 on page 46, and identifies five core capabilities within the Risk Assessment and Operations teams.



Figure 20: Hunter Team Composition [2]

The specific skill sets of the teams are [2]:

- Operating System/Applications Analyst - Analyze operating systems (Windows and Unix), applications (databases, directory services, mail servers, web, internal Domain Name Server (DNS)) for risks and compliance
- Boundary/Infrastructure Analyst - Analyze infrastructure (routers, switches, printers, file servers, etc.) and boundary (gateway, firewall, web, proxy, external DNS, wireless, etc.) for risks and compliance
- Traffic/Log Analyst - Analyze network traffic and logs from proxy, firewall and DNS for anomalous activity and indications
- Binary/Attack Vector Analyst - Perform malware analysis on anomalous executables and determine attack vector
- Mission Operator - Employs tool/Tactic Techniques and Procedures (TTPs) to defeat and/or mitigate cyberspace threats on targeted links, nodes and systems

5.1.4.3 Recommended CCS Team Composition: Stage 1 . The skill sets in section 5.1.4.2 outline a solid CND capability team. This researcher would however, recommend the team size of six increase to eight or nine to allow for more depth of expertise in the first two team functions. The Operating Systems function can become extremely complex between the two operating (Windows and Unix) systems and could warrant two separate experts. As well, the Applications analyst covers a broad range of functions that could require more than one team member. The Boundary/Infrastructure Analyst could also be split into more than one technician. For example, network backbone equipment [routers/switches] require a different knowledge than those of a firewall, web and/or wireless expert.

As far as covering the CNE training/personnel aspects of cyber operations, the same team in the 688 IOW Hunter team make-up discussed above would satisfy intelligence gathering, especially if CND actions “feed” directly into CNE products as correlated by General Matthews in section 4.4.2.

It is important to note, that all team member functions identified in the 688 IOW Hunter Team construct, with the exception of the Binary/Attack Vector Analyst and the Mission Operator, with little to no more additional training, already reside in a typical CCS. Most of these duties are needed to build and troubleshoot network services and are a core competency of the Airmen in a CCS. Therefore, in this researcher's opinion, the "Hunter" team is already at a minimum 75% mission Initial Operating Capability (IOC) in a CCS.

The recommended expanded 688 IOW Hunter Team composition for CND/E, as stage 1 for the CCS Hunter Team composition is displayed in Figure 21 on page 48

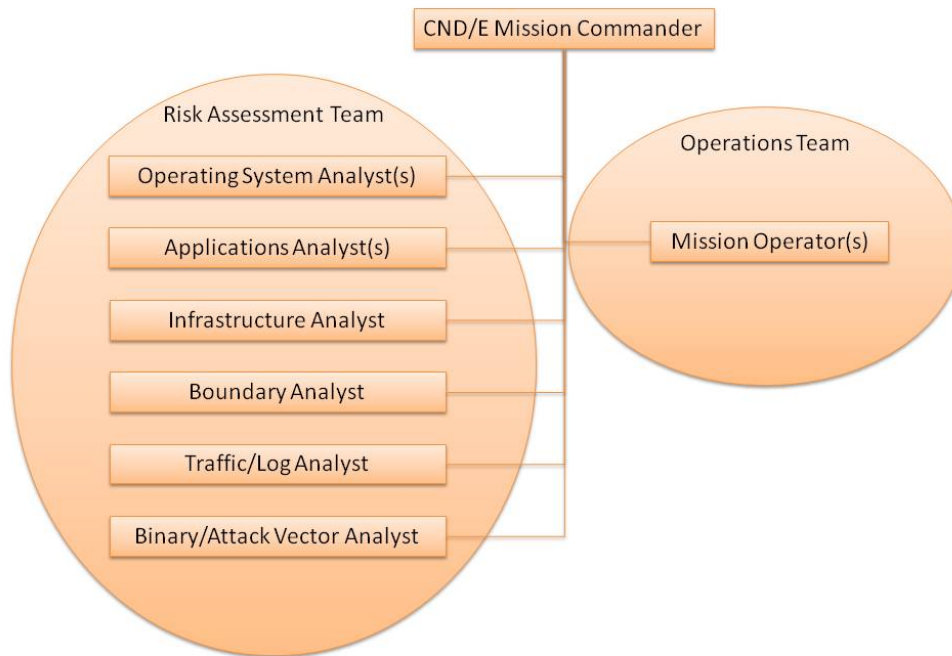


Figure 21: CCS Hunter Team Composition

5.1.4.4 *Recommended CCS Team Composition: Stage 2* . Robust employment of CNA activities, besides requiring more stringent legal authorities, warrant deeper thought for team composition. The stage 1, CSS Hunter team composition described above with the additional caveats [number of members and expansion from “Risk Assessment” to “*Risk and Vulnerability Exploitation Assessment Team*”] would make up a CNA team with an IOC, however this researcher would also recommend a few other skill sets to reach the 100% solution or Fully Operational Capability (FOC). The additional team members recommended are:

- Social Networking Expert - technician versed in current trends/methods of society interactions via networked (Internet), mobile media devices (smart phones) and the abilities to exploit (via technical infiltration) these modes of communication between target populations. This technician, could be the web expert, but should also work with the other Influence Operation team members (Psychological Operations), to ensure coordination and maximum efficiency of efforts.
- Electronic Disruption and Hijacking - technician versed in Electronic Warfare (EW) capabilities to influence wireless (network and/or cellular) nodes throughout the objective AOR. Again, this technician needs to be in sync with their Influence Operations team (EW) counterparts and could be satisfied with an EW expert with the necessary network skills.

The final recommended CNA/D/E package team composition, this researcher coined as the “*Cyber Hunt & Kill Team*”, completes stage 2. The CCS Cyber Hunt and Kill team is highlighted in Figure 22 on page 50.

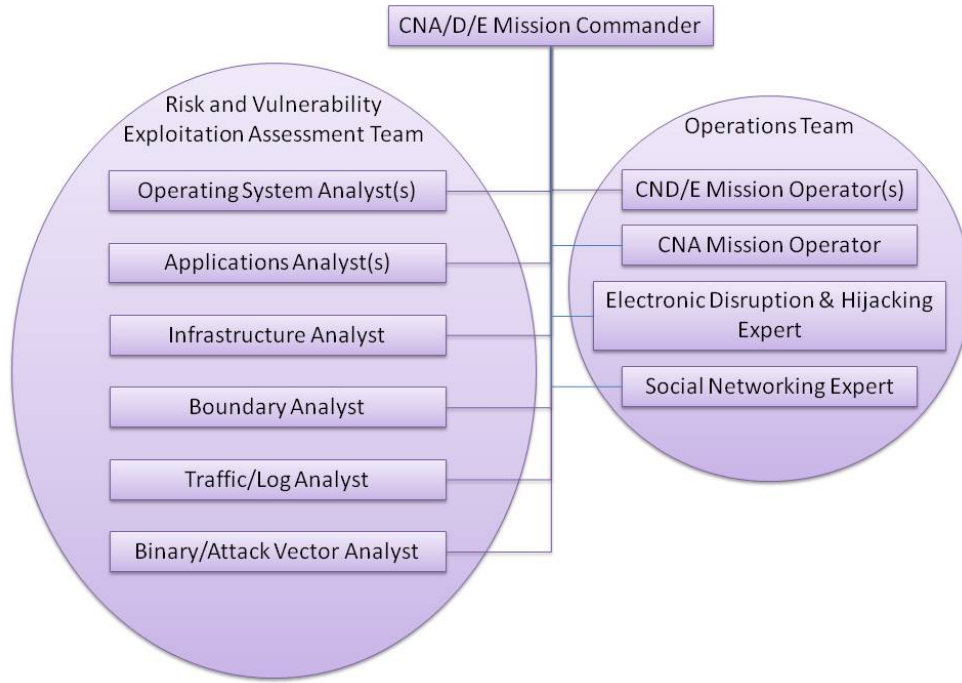


Figure 22: CCS Cyber Hunt & Kill Team Composition

5.1.5 Proposed Tool Sets. Selecting the correct “ordnance” for employment to avoid collateral damage and mitigate unwanted second and third order effects is the goal for all commanders in the field, and cyber operations are no exception.

[The] “Joint Forces will secure the “.mil” domain, requiring a resilient DOD cyberspace architecture that employs a combination of detection, deterrence, denial, and multi-layered defense. We will improve our cyberspace capabilities so they can often achieve significant and proportionate effects with *less cost and lower collateral impact.*” [10] Two of the interviewees in section 4.4 concurred the feasibility of precision munitions during cyber operations were a good idea, but foot-stomped the need to reduce the collateral effects induced during mission execution.

One way to attempt to minimize the collateral effects of cyber warfare is careful design of the munition being employed during the operation. The craftiness and thoroughness of design in computer viruses and worms has increased in sophistication over the past years. The W32.Stuxnet Dossier is a perfect example of a “targeted” com-

puter threat. “The ultimate goal of Stuxnet [was] to sabotage [the target] facility by reprogramming the programmable logic controllers (PLCs) to operate as the attackers intend them to, most likely out of their specified boundaries.” [3] The intended target for this worm were specific industrial control systems used to manage power plants. The Symantec Security Response team performed an extensive study of the Stuxnet worm. [3] In their research, in over 40,000 unique external network addresses from over 155 countries infected with the worm, 58% of the infected host systems resided in Iran. [3] The “infected system” breakout (by nations) from Symantec’s research is displayed in Figure 23 on page 51

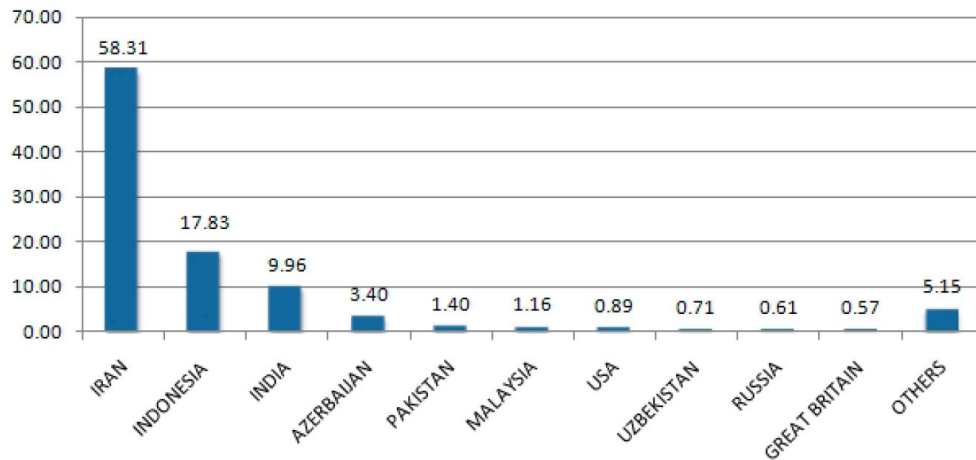


Figure 23: Geographic Distribution of Stuxnet Infections [3]

The creation of this worm took extensive planning and engineering and included aspects of “zero-day exploits, a Windows rootkit, the first ever PLC rootkit, antivirus evasion techniques, complex process injection and hooking code, network infection routines, peer-to-peer updates, and a command and control interface.” [3] Various tools like Stuxnet are needed in warfare to aid the commander in reaching mission objectives with the lowest possible chance of undesired results. The design of these munitions cannot, at this time, be mass produced to the like of a JDAM precision guided missile. Therefore, careful thought must be undertaken to the time and place of these *now* “strategic” weapons.

As technology advances, the high demand, low density of the precision cyber munitions will increase to the availability needed at the tactical battlefield. There are however, other options of cyber attack and active defense techniques still available to the commander to employ. One such tactic is to design military deception techniques as CND actions, such as hiding information about the network's topology, vulnerabilities, and assets from the attacker's ISR capabilities (e.g. scanning). As another tactic, a Honeypot ruse makes it difficult for hackers to find real networked assets such as files, logs and systems on the friendly networks. If designed and managed properly, a successful Honeypot can provide valuable intelligence and forensic information about the intruder and their method of attack. [34]

Additionally, more routine hacker techniques [for example, web site defacement/alteration, web site redirections through friendly nodes for monitoring/interception, cellular device jamming/interceptions] can be used without "tipping the hand" of current CNA/E capabilities now held by friendly forces that will minimize the collateral damage possibilities. However, as all actions executed in the battlefield, proper coordination and planning is key to over-arching success of all the Nation's objectives.

This Air Force cyber coordination at the Joint Task Force/COCOM level of operations, is currently under the responsibility of the Air Component Coordination Element (ACCE) assigned to USCYBERCOM and the Cyber Operations Liaison Elements (COLE) assigned in a theater Air Operations Centers (AOC) at each of the Component Numbered Air Forces (C-NAF). "The ACCE serves as the 24 AF/CCs personal representative to the Commander of USCYBERCOM and will provide AF Cyber expertise through direct liaison and reach-back to the USCYBERCOM staff". The COLE is "modeled after the Special Operations Liaison Element concept and is envisioned to inject Cyber expertise at the point of synchronization." [1] The C2 and coordination lines for these two functions during joint operations is detailed in Figure 24 on page 53

5.1.6 Time Phased Implementation.

5.1.6.1 1 to 3 Years:. To implement these capabilities will take time, planning and focused training. To get the first CCS cyber competency in the field for the commander, this researcher recommends to begin with 688 IOW Hunter team partnerships and focus on CND in regards to mission assurance. First, fold the 688 IOW Hunter Teams into the CSS as suggested by Col Giorlando in section 4.4.4 to satisfy any existing requirements the warfighter might currently need. Then, following the same training regiment of the 688 IOW Hunter Teams, subject a cadre of CCS personnel to complete the defense specific curriculum. The number of CCS defense teams should be dependent of, but at least equal to, the number of CCSs the COCOMS currently require for a deployed capability.

5.1.6.2 3 to 6 Years:. At this point, CCSs should now possess the stand alone CND capability and can begin to roll in CNE formally into their arsenal. Close coordination, information sharing, and partnerships with intelligence communities in theater and in garrison (NSA) is critical for a robust CNE resource for the commander. Additionally, as a deployed partner to the 688 IOW Hunter Teams, the CCSs can also augment the CND mission assurance capability AFNet-wide, in garrison or in a deployed environment. This eliminates the current three-team “short-fall” of the Hunter Team capacity highlighted in section 5.1.4.1 as well as enables a continued defense against any adversary’s active persistent threat discussed in Col Skinner’s interview in section 4.4.3.

5.1.6.3 6 to 10 Years:. By this time, the age of cyber warfare will have materialized past a buzz-word into a full fledged capability nations [and non-state actors] employ in concert with other combat resources. Furthermore, the AETC training programs and opportunities should be mature enough to provide the Air Force an abundant and constant pipeline of cyber warriors trained in the art of attack, thus completing the CCS transformation with complete CNA for the deployed warfighter.

CCSs should now be able to perform the full spectrum of cyber operations, *computer network attack, computer network defense and computer network exploitation*.

5.2 Final Thoughts and Challenges

The following are some final thoughts and challenges Air Force leaders should consider to guarantee success in the Nation's future contingencies and conflicts involving and relying on cyberspace as a force multiplier. As seen in some of the "common themes" in section 4.3.3, the capability of CND at the on-site tactical level is shared amongst both sides of the respondents polled. Therefore, if no other on-site cyber capability makes it to the field, CND must be the exception. DOD has already succumbed to the fact the complete defense of the GIG is an insurmountable task, however this does not mean that the warfighter should not secure as many of the portions of the GIG as possible, allowing the defensive cascade to encompass mission critical operations.

Another theme worth mentioning is the level of expertise needed to learn and maintain proficiency in cyber warfare. These tools, tactics techniques and procedures are not easily obtained and mastered and unlike their air power counterparts rapidly change. The Air Force should consider acquisition strategies, training programs and personnel retention plans to meet this challenging domain. This researcher also recommends adopting the same (or similar) service commitment and assignment considerations as the Air Force's pilots currently agree to. After the cyber Airmen completes their training, the Air Force should establish a 8-10 year service commitment (with similar bonuses) and continue to place the cyber warrior in jobs that would fully utilize their experience throughout their first 8-10 years of service (at a minimum). It must be recognized that these highly trained personnel are, and will continue to be very marketable in the civilian sector. Their skills take time to master and demand continual refinement and proper employment.

Finally, the theme at the top of the list, is the perception of the level of awareness the strategic (military or civilian) leaders lack in cyber operations. Just as the

employment of air power required education, proof of competence and impact in the conflict, and most importantly a level of comfort in the tools, the benefit of air power took leaders time to understand and accept. This researcher recommends, training senior leaders on the benefits of this new force multiplier just as much as training the forces to employ the capability. There are educational prospects to train AF leaders in the IDE and Senior Developmental Education military programs. However, at a minimum, the DOD should consider the opportunity to deliver an extensive training block in the Joint Forces Staff College (JFSC). JFSC is responsible in training senior leaders in Joint Operations and is a prerequisite to becoming a General Officer, who some of which will become a Joint Force Commander at some point in their career. Bottom-line, the most experienced and trained warrior, wielding the most advanced weaponry cannot impact the outcome in the battlefield if they are not used at the right place and time for maximum efficiency and effectiveness.

VI. Conclusions

“The Air Force ensures it can establish and maintain cyberspace superiority and fight through cyberspace attacks at any time regardless if the US requires the use of military forces.” [17]

The road from network assurance to mission assurance will take a continued level of commitment and thoughtful understanding. Some of the complexity comes to bear because the cyber domain is a global, 24 hour, 365 day domain and must be ready to support a commander in any AOR throughout the world at any moment. Unlike in the air domain, where air superiority is achieved at a certain point in an operation in a given AOR, cyber “superiority” must be at an acceptable level at all times globally.

However, AFDD 3-12 does point out that “just as in the air domain, we do not defend the entire cyberspace domain; we defend what is relevant to our operations”. [17] This is true, but, just as the aircraft have to be ready for flight, the satellite in the correct orbit and location, or the Airman trained and at the ready for a deployment when the call comes, so must DODs slice of cyberspace be ready to serve the Nation.

AF doctrine also explains that decentralized execution in the air domain is preferred to the down range commander for flexibility, timeliness, etc. So, although the cyber back-bone affords the opportunity to reach out across the world at light speeds, there may be instances when it is not possible for remote execution. For example, the back-bone might become severed, or it is not yet connected to the AOR due to deployed operations or the visibility into the adversaries’ networks is not evident to the remote site and therefore, vulnerabilities cannot be exploited for the benefit of the Joint Force Commander’s mission.

The research showed that two thirds of the AF population surveyed believe there should be a deployed cyber capability for the commander’s discretionary use during contingency operations. There are challenges in creating and sustaining this decentralized on-site computer network attack, defense and exploitation force for the commander, but these challenges are not insurmountable. The data collected by the survey and interviews conducted along with this researcher’s recommendations

map out a solid team composition and implementation time-line to develop the new capabilities in a combat communication squadron.

In conclusion, cyber operations should not trickle from the bottom-up or be an after thought during planning and operations. Cyber operations must an equal with land, sea, air and space operations and available to the Joint Force Commander. In the end, when the military receives the call to go into action, it is time to *Be Ready to Get the Job Done*.

Bibliography

1. USAF Space Command, “24 Air Force Service Cyber Capability / Forces,” Mar 2011.
2. USAF Space Command, “Operating Concept for Hunter Teams (Phase 1),” Feb 2010.
3. Nicolas Falliere, Liam O Murchu, and Eric Chien, “W32.Stuxnet Dossier,” Feb 2011. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.
4. DoD, “Joint Publication 3-30, Command and Control for Joint Air Operations,” Jan 2010.
5. DoD, “Joint Publication 1-0, Doctrine for the Armed Forces of the United States,” Mar 2009.
6. Dr. Mills, Robert, “Instruments of National Power - aka the “Means”,” AFIT/ENG, 2011.
7. DoD, “Joint Publication 3-13, Information Operations,” Feb 2006.
8. DoD, “Joint Publication 1-02, Department of Defense Dictionary of Military and Associated Terms,” Apr 2010.
9. Dept of Defense , “Joint Publication 6-0, Joint Communications System,” June 2010.
10. Chairman, Joint Chiefs of Staff, “National Military Strategy of the United States of America,” Feb 2011.
11. DOD, “Quadrennial Defense Review Report,” Feb 2010.
12. Maj Bledstein, Noah , “Legal Considerations in Cyber Operations Brief,” Feb 2011.
13. Dept of Defense, “Joint Publication 3-33, Joint Task Force Headquarters,” Feb 2007.
14. L. J. Janczewski and A. M. Colarik, *Cyber Warfare and Cyber Terrorism*, Information Science Reference, 2008.
15. Dept of Homeland Security, “The National Strategy to Secure Cyberspace,” Feb 2003.
16. M. Libicki, *Cyberdeterrence and Cyberwar*, RAND, 2009.
17. USAF, “Air Force Doctrine Document 3-12, Cyberspace Operations,” July 2010.
18. USAF, “Air Force Doctrine Document 2-5, Information Operations,” Jan 2005.

19. Dept of Defense, "DODI 8500.2, Information Assurance (IA) Implementation," Feb 2003. <http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>.
20. Dept of Defense, "DODI 3020.40, DoD Policy and Responsibilities for Critical Infrastructure," July 2010. http://www.fas.org/irp/doddir/dod/d3020_40.pdf.
21. Clark, Kevin P. and Jet Propulsion Laboratory, "Mars Global Surveyor Mission Assurance: Key Approaches for Faster, Better, Cheaper Missions," *IEEE*, pp. 491–506, 1998.
22. Maj. Gen. Webber, Richard E., Commander, 24th AF, "Air Force Cyber Numbered Air Force Achieves Initial Operational Capability," Jan 2010. <http://www.af.mil/news/story.asp?id=123187145>.
23. Dept of Defense, "Joint Publication 3-0, Joint Operations," Mar 2010.
24. Lt Gen Hobbins, William, USAF, "Airmen on the Battlefield: Warfighting Integration in Support of Special Operations Forces," *Air and Space Power Journal*, Spring 2005.
25. Dept of Defense, "Quadrennial Roles and Missions Review Report," Jan 2009. http://www.defense.gov/news/Jan2009/QRMFinalReport_v26Jan.pdf.
26. Mr. Wachdorf, Art, 24 AF/CA, "Challenges to AF Cyber Operations," AFCEA, 2010. http://www.afceaeriecanal.com/Info_Challenges_Brief_Jun_10.pdf.
27. AFCEA, "Defending America - CYBERSPACE 2011," AFCEA, 2011. http://www.afcea.org/calendar/eventdet.jsp?event_id=21380&w=N.
28. Capt Johnson, 333 TRS, AETC, "Bullet Background Paper on Undergraduate Cyber Training (UCT)," Aug 2010.
29. MSgt Matute, 333 TRS, AETC, "Bullet Background Paper on 1B4X1 - Cyberspace Defensive Operations," Jan 2011.
30. Capt Blacke, AFSPC/PA, "Intermediate network warfare training up and running," Mar 2011. <http://www.af.mil/news/story.asp?id=123245038>.
31. AFIT Electrical and Computer Engineering Dept, "Cyber Operations (MS) Degree Program," <http://www.afit.edu/EN/eng/cyberoperationsms.cfm>.
32. AFIT Electrical and Computer Engineering Dept, "Cyber Warfare (ICW), Intermediate Developmental Education (IDE) Cyber War Program," <http://www.afit.edu/en/eng/cyberwarfare.cfm>.
33. "Air Force Manpower and Equipment Force Packaging System, 6KTEB, C, D, etc UTCs and Mission Capability statements,"
34. Yuill, James J., "DEFENSIVE COMPUTER-SECURITY DECEPTION OPERATIONS: PROCESSES, PRINCIPLES AND TECHNIQUES," 2006. <http://www4.ncsu.edu/~jjyuill/yuill-thesis.pdf>.

35. US Army War College, "Information Operations Primer," Nov 2010. <http://www.carlisle.army.mil/usawc/dmspo/Publications/Information%20operations%20Primer%20AY11%20Web%20Version.pdf>.
36. USAF, "Air Education & Education Training Welcome Page," <http://www.aetc.af.mil/main/welcome.asp>.
37. USAF, "AIR FORCE INSTRUCTION 33-115, VOLUME 1," May 2006. <http://www.af.mil/shared/media/epubs/AFI33-115V1.pdf>.

Appendix A. Interviewee's Public Release Statements

A.1 Col Giorlando's Interview Release Statement



**DEPARTMENT OF THE AIR FORCE
689TH COMBAT COMMUNICATIONS WING (AFSPC)
ROBINS AIR FORCE BASE, GEORGIA 31098-2236**

MEMORANDUM FOR RECORD

FROM: 689 CCW/CC

SUBJECT: Interview Public Release Statement

1. The views expressed in the Section 4.4 of Major Michael Myers' Graduate Research Paper, "Emerging Roles of Combat Communication Squadrons in Cyber Warfare as Related to Computer Network Attack, Defense and Exploitation" are a correct dictation of the interview conducted by Major Myers for his research and has not been used out of context. The information provided details my experiences and thoughts related to this topic of research. The information is true and correct as written and does not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government. I hereby grant permission for my interview to be included as a part of this research and available for public release.
3. If you have any questions, please contact my Executive Officer, Capt Andrew Miller, at 472-8689.

A handwritten signature in black ink, appearing to read "Theresa Giorlando", is positioned above the printed name.

THERESA GIORLANDO, Colonel, USAF
Commander

A.2 Col Gardiner's Interview Release Statement




DEPARTMENT OF THE AIR FORCE HEADQUARTERS AIR FORCE SPECIAL OPERATIONS COMMAND

MEMORANDUM FOR RECORD

FROM: AFSOC/A6
100 Bartley St., Suite 137E
Hurlburt Field FL 32544

SUBJECT: Interview public release statement

The views expressed in the Section 4.4 of Major Michael Myers' Graduate Research Paper, "Emerging Roles of Combat Communications Squadrons in Cyber Warfare as Related to Computer Network Attack, Defense and Exploitation" are a correct dictation of the interview conducted by Maj Myers for his research and has not been used out of context. The information provided, details my experiences and thoughts related to this topic of research. The information is true and correct as written and does not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government. I hereby grant permission for my interview to be included as a part of this research and available for public release.


VON A. GARDINER, Colonel, USAF
Director, Communications and Information

A.3 Col Skinner's Interview Release Statement



DEPARTMENT OF THE AIR FORCE
688TH INFORMATION OPERATIONS WING (AFSPC)
LACKLAND AIR FORCE BASE TEXAS

JUN 02 2011

MEMORANDUM FOR RECORD

FROM: ROBERT J. SKINNER
688 IOW/CC

SUBJECT: Interview Release for Major Myers' Graduate Research Paper

The views expressed in the Section 4.4 of Major Michael Myers' Graduate Research Paper, "Emerging Roles of Combat Communications Squadrons in Cyber Warfare as Related to Computer Network Attack, Defense and Exploitation" are a correct dictation of the interview conducted by Maj Myers for his research and has not been used out of context.

The information provided details my experiences and thoughts related to this topic of research. The information is true and correct as written and does not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government. I hereby grant permission for my interview to be included as a part of this research and available for public release.

A handwritten signature in black ink, reading "Robert J. Skinner", is positioned above the printed name.

ROBERT J. SKINNER, Colonel, USAF
Commander

A.4 Gen Matthew's Interview Release Statement



UNITED STATES TRANSPORTATION COMMAND

508 SCOTT DRIVE
SCOTT AIR FORCE BASE, ILLINOIS 62225-5357

JUN 08 2011

MEMORANDUM FOR GRADUATE ACADEMIC PANEL

FROM: USTRANSCOM/TCJ6

SUBJ: Consent for Public Release of Research Paper



The views expressed in the Section 4.4 of Major Michael Myers' Graduate Research Paper, "Emerging Roles of Combat Communications Squadrons in Cyber Warfare as Related to Computer Network Attack, Defense and Exploitation" are a correct dictation of the interview conducted by Maj Myers for his research and has not been used out of context. The information provided, details my experiences and thoughts related to this topic of research. The information is true and correct as written and does not reflect the official policy or position of the United States Air Force, the Department of Defense, or the United States Government.

I hereby grant permission for my interview to be included as a part of this research and available for public release.

A handwritten signature in black ink, appearing to read "Earl D. Matthews", is positioned above the typed name.

EARL D. MATTHEWS
Brigadier General, USAF
Director, Command, Control,
Communications, and Computer Systems

Appendix B. Survey Questions



AIR FORCE INSTITUTE OF TECHNOLOGY **689th CCW/CC Survey**

Survey Control Number: DAFA6011-028

Privacy Notice

The following information is provided as required by the Privacy Act of 1974:

Purpose: Thank you for participating in this short survey. On behalf of the 689 CCW/CC, I am researching the emerging role of Combat Communications units in relation to computer network attack¹, defense², and exploitation³ (CNA/D/E).

Participation: We would greatly appreciate your participation in our data collection effort. In this research I will analyze how the combat communication unit's mission is evolving from network assurance to mission assurance. As Air Force missions increase their reliance on the network so must the focus of communication units change. This survey will contribute to my research towards determining what you have experienced in previous deployments with how the Air Force is reorganizing communication squadrons and AFSCs towards ensuring the freedom to operate in the cyber domain.
Your participation is **COMPLETELY VOLUNTARY**.

Confidentiality: We ask for some demographic information in order to interpret results more accurately. **ALL ANSWERS ARE ANONYMOUS.** No one other than the research team will see your completed questionnaire. If you have any additional information that you think will contribute towards this research please include it at the end of the survey.

¹**Computer network attack (CNA).** Actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. (JP 3-13)

²**Computer network defense (CND).** Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense information systems and computer networks. (JP 6-0)

³**Computer network exploitation (CNE).** Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks. (JP 1-02)

Instructions

- Base your answers on your own thoughts & experiences
- Please make your answers clear and concise when asked to answer in a response or when providing comments
- Be sure to select the correct option button when asked
- Please keep your responses unclassified.

Contact information:

If you have any questions or comments about the survey, contact **Maj Michael Myers** at the number, fax, mailing address, or e-mail address listed below.

AFIT/ENV BLDG 640 / Room 104A
2950 Hobson Way
Wright-Patterson AFB, OH 45433-7765
Email: Michael.Myers@afit.edu
Advisor: Michael.Grimaila@afit.edu
Phone: DSN 785-3636x7395, commercial (937) 255-3636x7395
Fax: DSN 986-4699; commercial (937) 656-4699

Start Survey

Section I:

If you answer "NO", you will be redirected to the next question

| | | Yes | No |
|---|--|-----------------------|-----------------------|
| | | 1 | 2 |
| 1 | Have you been deployed (one or more times) with a tactical communications unit to support a contingency commander ⁴ ? | <input type="radio"/> | <input type="radio"/> |

⁴ Commander in this survey means either Joint Task Force (JTF) commander or similar commander in charge of entire contingency, not necessarily your immediate commander.

Continue

A. In any of the above deployments did your unit support the commander ⁴ in a following capacity:

| 1a | | Yes | No |
|----|------|-----------------------|-----------------------|
| | | 1 | 2 |
| 1 | CNA. | <input type="radio"/> | <input type="radio"/> |
| 2 | CND. | <input type="radio"/> | <input type="radio"/> |
| 3 | CNE. | <input type="radio"/> | <input type="radio"/> |

B. In any of the above deployments do you feel your unit should have supported the commander ⁴ in a following capacity:

| 1b | | Yes | No |
|----|------|-----------------------|-----------------------|
| | | 1 | 2 |
| 1 | CNA. | <input type="radio"/> | <input type="radio"/> |
| 2 | CND. | <input type="radio"/> | <input type="radio"/> |
| 3 | CNE. | <input type="radio"/> | <input type="radio"/> |

⁴ Commander in this survey means either Joint Task Force (JTF) commander or similar commander in charge of entire contingency, not necessarily your immediate commander.

Continue

C. If you answered "Yes" to any part of question 1.b, what was the reason your unit did not perform a CNA/D/E action to support the commander? Please select one or more reasons below and rank their importance.

| 1 c | | N/A | Somewhat Important | Important | Very Important |
|-----|--|-----------------------|-----------------------|-----------------------|-----------------------|
| | | 1 | 2 | 3 | 4 |
| 1 | Policy, ROE, etc. (If "Policy, ROE", what level: National, HHQ, Local, etc.) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | | <input type="text"/> | | | |
| 2 | Legal (If "Legal", Please Explain) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | | <input type="text"/> | | | |
| 3 | Lack of training in one or more of the CNA/D/E fields (If "Lack of Training", Which field?) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | | <input type="text"/> | | | |
| 4 | Other (If "Other", Please Explain) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | | <input type="text"/> | | | |

D. To your knowledge, did any other unit support the commander in any of the CNA/D/E actions?

| 1 d | | Yes | No |
|-----|--|-----------------------|-----------------------|
| | | 1 | 2 |
| 1 | If Unsure (Includes Cannot Comment), select NO | <input type="radio"/> | <input type="radio"/> |
| 2 | Can you indicate what type of Unit? (If, 'Yes', what type of unit?) | <input type="radio"/> | <input type="radio"/> |
| | | <input type="text"/> | |
| 3 | Did they perform any actions? (If "Yes", What action did they perform?) | <input type="radio"/> | <input type="radio"/> |
| | | <input type="text"/> | |

E. What was your position/role in the deployed environment and rank at the time(s) of those deployment(s) (last 3)?

| 1 e | | | |
|------------|----------------------|--------|----------------------|
| Position 1 | <input type="text"/> | Rank 1 | <input type="text"/> |
| Position 2 | <input type="text"/> | Rank 2 | <input type="text"/> |
| Position 3 | <input type="text"/> | Rank 3 | <input type="text"/> |

⁴ Commander in this survey means either Joint Task Force (JTF) commander or similar commander in charge of entire contingency, not necessarily your immediate commander.

| | | Yes | No |
|---|---|----------------------------------|-----------------------|
| | | 1 | 2 |
| 2 | Do you feel it is necessary for the supported commander to have the option to employ any of the CNA/D/E actions at the tactical level by a deployed tactical unit?. | <input checked="" type="radio"/> | <input type="radio"/> |

You answered "Yes". What do you believe the barriers are? Please select one or more reasons below and rank their importance.

| 2 A | | N/A | Somewhat Important | Important | Very Important |
|-----|---|-----------------------|-----------------------|-----------------------|-----------------------|
| | | 1 | 2 | 3 | 4 |
| 1a | Policy, ROE, etc. <i>(If "Policy, ROE", what level: National, HHQ, Local, etc.)</i> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | | | | | |
| 2a | Legal <i>(If "Legal", Please Explain)</i> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | | | | | |
| 3a | Lack of training in one or more of the CNA/D/E fields <i>(If "Lack of Training", Which field?)</i> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | | | | | |
| 4a | Other <i>(If "Other", Please Explain)</i> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | | | | | |

You answered "No", what is your rationale? Please select one or more reasons below and rank their importance.

| 2 B | | N/A | Somewhat Important | Important | Very Important |
|-----|--|-----------------------|-----------------------|-----------------------|-----------------------|
| | | 1 | 2 | 3 | 4 |
| 1 | Already happens remotely from other units <i>(which one if you can say)</i> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | | | | | |
| 2 | Not a deployed tactical unit's mission <i>Please Explain</i> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | | | | | |
| 3 | Policy, ROE, etc. <i>(what level: National, HHQ, Local, etc.)</i> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | | | | | |
| 4 | Legal <i>(If "Legal", Please Explain)</i> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | | | | | |
| 5 | Lack of training in one or more of the CNA/D/E fields <i>(which field?)</i> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | | | | | |
| 6 | Other <i>(If "Other", Please Explain)</i> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| | | | | | |

| | | | |
|---|--|-----------------------|-----------------------|
| | | Yes | No |
| | | 1 | 2 |
| 3 | Are you retired from military, or civilian service?. | <input type="radio"/> | <input type="radio"/> |

You answered "Yes", Please check the rank you retired at then indicate your current position (i.e. company Chief Technical Officer, government advisor, etc).

| | | | | | | |
|----|---------------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| | E1 – E6 | E7 – E9 | O1 – O3 | O4 – O6 | O7+ | Civilian |
| | 1 | 2 | 3 | 4 | 5 | 6 |
| 3b | Rank retired. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

| | | |
|----|--------------|----------------------|
| 3b | Position Now | <input type="text"/> |
|----|--------------|----------------------|

You answered "No", What is your current position and rank?

| | | | | | | |
|----|---------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| | E1 – E6 | E7 – E9 | O1 – O3 | O4 – O6 | O7+ | Civilian |
| | 1 | 2 | 3 | 4 | 5 | 6 |
| 3a | Rank. | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

| | | |
|----|----------|----------------------|
| 3b | Position | <input type="text"/> |
|----|----------|----------------------|

| | | |
|---|--|-----------------------|
| | A6 | A3 |
| | 1 | 2 |
| 4 | Is your experience primarily in the A6 (communications) or A3 (operations) community?. | <input type="radio"/> |

| | | |
|---|-------------------------------------|----------------------|
| 5 | Additional Information to consider. | <input type="text"/> |
|---|-------------------------------------|----------------------|

FINISH

Appendix C. Referenced Unit Mission Descriptions

The missions of U.S. Strategic Command (USSTRATCOM) are to deter attacks on U.S. vital interests, to ensure U.S. freedom of action in space and cyberspace, to deliver integrated kinetic and non-kinetic effects to include nuclear and information operations in support of U.S. Joint Force Commander operations, to synchronize global missile defense plans and operations, to synchronize regional combating of weapons of mass destruction plans, to provide integrated surveillance and reconnaissance allocation recommendations to the SECDEF, and to advocate for capabilities as assigned. [35]

The U.S. Cyber Command (USCYBERCOM) located in Fort Meade, MD plans, coordinates, integrates, synchronizes, and conducts activities to: direct the operations and defense of specified Department of Defense information networks and; prepare to, and when directed, conduct full-spectrum military cyberspace operations in order to enable actions in all domains, ensure US/Allied freedom of action in cyberspace and deny the same to our adversaries. [35]

The National Security Agency/Central Security Service (NSA/CSS) has two main missions. The Signals Intelligence (SIGINT) mission allows for an effective, unified organization and control of all foreign signals collection and processing activities of the U.S. The NSA/CSS is authorized to produce SIGINT in accordance with the objectives and priorities established by the Director of National Intelligence in consultation with the President's Foreign Intelligence Advisory Board. Foreign signals collection is a Title 50 United States Code (USC) authority given to the Director, NSA/CSS. The Information Assurance (IA) mission provides the IA and Computer Network Defense (CND) solutions/services, and conducts Defensive Information Operations (DIO) in order to protect information processed by U.S. national security systems. The intent is to measurably improve the security of critical operations and information by providing know-how and technology to our suppliers, partners and

clients, when and where they need them. The NSA/CSSs IA mission is authorized by National Security Directive 42. [35]

Air Force Space Command (AFSPC) was assigned the Cyber mission (transferred from Air Combat Command) when 24 AF was established on 18 August 2009. AFSPC is 24 AFs “Organize, Train and Equip” entity which advocates for personnel funding training and equipment to support the mission areas to enable 24 AF to meet operational mission requirements. AFSPC also provides administrative support, audit and inspections, financial management, manpower and organization, operational analysis, research and development, and training and education support to 24 AF. [35]

Air Force Education & Training Command (AETC) Air Education and Training Command, with headquarters at Randolph Air Force Base near San Antonio, Texas, was established July 1, 1993, with the realignment of Air Training Command and Air University. AETC’s role makes it the first command to touch the life of almost every Air Force member. AETC’s mission is to develop America’s Airmen today... for tomorrow. [36]

The 24th Air Force (24 AF) is located at Lackland AFB, TX and has three subordinate wings, the 67th Network Warfare Wing (67 NWW), located at Lackland AFB, TX, the 688th Information Operations Wing (688 IOW), also located at Lackland AFB, TX, and the 689th Combat Communications Wing (689 CCW) at Robins AFB, Georgia. Specifically, the 24 AF mission is to: Extend, operate and defend the Air Force portion of the DOD network and to provide full spectrum capabilities for the Joint warfighter in through and from Cyberspace [1], [35]

The 624th Operations Center (624 OC), collocated with the 24 AF at Lackland AFB, TX serves as the 24 AF’s command and control center to provide a robust full-spectrum and integrated Cyberspace operations capability. The 624 OC interfaces with United States Cyber Command (USCYBERCOM) and theater and functional Air Operations Centers to establish, plan, direct, coordinate, assess, and command & control Cyber operations in support of AF and Joint warfighting requirements. [1]

The 67 NWW is charged as the Air Force execution element for Air Force Network Operations and providing network warfare capabilities to Air Force, Joint Task Force and combatant commanders that operate, manage, and defend global Air Force networks. Additionally, the 67 NWW performs electronic systems security assessments for the Air Force and Joint community. As the Air Force's only network warfare wing, it has Airmen around the world conducting and supporting Cyber operations. The wing is composed of three groups, 12 squadrons, one flight, and several detachments with more than 2,000 Airmen and contractors executing the Cyber portion of the Air Force mission. [1]

The 688 IOW delivers proven Information Operations, Engineering and Infrastructure capabilities integrated across air, space and cyberspace. The wing is comprised of two groups: the 318th Information Operations Group (318 IOG) and the 38th Cyberspace Engineering Group (38 CEG). The 318 IOG is the Air Force's center of excellence for information operations. They are responsible for creating the information operations advantage for combatant forces through exploring, developing, applying and transitioning counter information technology, strategy, tactics and data to control the information battlespace. In addition, the 318 IOG trains Airmen in Network Warfare skills, Information Operations, and develops Mission Qualification Training for 67 NWW units. The 38 CEG is the Air Force's premier Engineering Installation Group providing engineering solutions to customers world-wide at every level of command. [1]

The 689 CCW delivers combat communications for the joint and coalition warfighter supporting combat operations and Humanitarian Relief Operations. The wing has a total-service wartime capability that encompasses more than 600 million dollars worth of material and 50 Air Force units comprised of almost 1,500 active duty Airmen who provide combat communications and Air Traffic Control and Landing Systems capabilities in the Continental United States and Abroad. The combat communications mission also includes the greatest portion of 24 AFs aligned reserve component, with over 6,000 aligned Air Guard and Reserve members. [1]

The Integrated Network Operations and Security Center (I-NOSC) perform work done at present MAJCOM NOSC under the command of the AFNETOPS/CC. These regional I-NOSCs give commanders visibility into the network to achieve operational objectives. I-NOSCs must establish the ability to provide commanders a real time presentation of their network forces. Within their theater, each I-NOSC manages functions currently performed by MAJCOM NOSC i.e., network defense; generates an enterprise situational awareness picture; manages network configuration; and provides information assurance and Spectrum management. This includes voice, video, and data networks supported by the GIG. [37]

Appendix D. Researcher's Vita

Maj Michael Myers

michael.myers.7@us.af.mil

CAREER PROFILE

Results-oriented Air Force Communications Officer with a strong background in leadership, information systems administration, project management and customer service. Skilled at building, leading and motivating high performing teams in delivering outstanding levels of productivity. Ability to perform in an environment of high pressure where decisions are made at a fast pace and are critical to the survival of personnel. Accomplished communicator, with ability to liaise with all levels of management and deliver presentations to groups of diverse sizes and backgrounds. Proven leader in achieving immediate and long-term goals while meeting operational deadlines in high paced, high stress environment.

PROFESSIONAL EXPERIENCE

UNITED STATES AIR FORCE 1999 to Present

Graduate Student, Air Force Institute of Technology (AFIT) 2010 to Present

Currently attending the Air Force Institute of Technology for a Master of Science in Cyber Warfare with a concentration of study in cyberspace operations and information operations functions and activities including network attack (Net-A), network defense (Net-D), network warfare support (NS), network operations and related information operations in support of joint, national and AF objectives.

Project Manager, NORAD and NORTHCOM (N-NC) 2008 to 2010

Performed a Joint tour at NORAD and NORTHCOM (N-NC) on Petersen AFB, CO as the J6 Portfolio manager for all command deployable C2 communications projects. Led 9 Project Managers directing complete management of projects worth \$30M+. While at N-NC, he completed the JPME II course at Norfolk, VA and is now Joint Service Officer qualified.

Director of Operations/Flight Commander, Anderson AFB 2005 to 2008

Performed director of operation duties in the 644 CBCS for five months and designed 5 MILCON facilities worth over \$12M. Developed and executed a roadmap leading to the squadrons Initial Operations Capability in June 08.

Base network flight commander at 36th CS. Led a team of 100 enlisted, civilians and contractors providing core network services with assets valued at \$20M. Directed the Network Control Center, automated data processing equipment, wing information assurance, and communications security (COMSEC) requirements for 4K base personnel.

Budget Analyst/Branch Chief, Scott AFB 2002 to 2005

Lead budget analyst in ECVN (Enterprise Capabilities Voice Networks) for five Lead Command Programs, including Combat Information Transport System (CITS). Provided fiscal POM and financial planning documents totaling over three billion dollars during the current FYDP to the Air Force Corporate Structure. Additionally, appointed as Branch Chief of ECVN within the CITS lead command to provide Air Force-level management for over 360 voice switching and cabling systems valued at \$2.1 billion providing essential capabilities to execute Global Engagement missions.

Group Executive Officer/Network Control Center (NCC) OIC, Barksdale AFB 1999 to 2002

Performed Support Group Executive Officer duties over five wing squadrons and led the Network Control Center (NCC) as Officer in Charge OIC.

| UNITED STATES NAVY 1987 to 1999 |

Engineering Aid, US Navy Seabees, Naval Mobile Construction Battalions 1987 to 1999

As a Seabee, gained extensive knowledge in construction practices, management and quality control. Deployments include Operation DESERT SHIELD/STORM and

on a Civic Action Team sent to the Fiji Islands for typhoon disaster relief. Additionally, performed duties as a Navy law enforcement officer.

Construction experience in: planning, supervising, and performing tasks required in construction surveying, drafting, planning and estimating, and quality control including: traces and revises drawings; prepares construction drawings and architectural layouts; performs field sanitation procedures; places construction stakes and other references; uses standard surveying instruments; performs simple tests on soils and concrete materials; draws detailed electrical and mechanical drawings of service utilities and distribution/collection systems; draws detailed civil, architectural, and structural drawings; prepares materials requisitions; records survey field notes; inspects the placing of concrete and tests its compressive and flexural strength; prepares topographic maps; conducts tests and performs field adjustments on survey equipment; tests for soil compaction field density, Atterberg limits, and aggregate soundness.

EDUCATION

- 1997: Bachelor of Science in Computer Information Systems, University of West Florida, Pensacola, FL
- 1999: Officer Training School, Maxwell AFB, AL
- 1999: Basic Communication Officers Training (residence), Keesler AFB, MS
- 1999: Aerospace Basic Course (residence), Maxwell AFB, AL
- 2001: Masters of Science in Systems Technology, Louisiana State University, Shreveport, LA
- 2004: Squadron Officer School (residence), Maxwell AFB, AL
- 2008: Advanced Communication Officers Training (residence), Keesler AFB, MS
- 2009: JPME I, Air Force Command and Staff College (correspondence)

- 2009: JPME II, Joint Forces Staff College (residence), Norfolk, VA
- 2010: AFIT Cyber Warfare, Masters of Science (current)

AWARDS

- Defense Meritorious Service Medal
- Air Force Meritorious Service Medal with one device
- Air Force Commendation Medal with one device
- Navy Good Conduct Medal with two devices

| REPORT DOCUMENTATION PAGE | | | | | Form Approved OMB No. 0704-0188 | |
|--|-------------|---------------------------|----------------------------|--|--|--------------------------|
| <p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</p> | | | | | | |
| 1. REPORT DATE (DD-MM-YYYY) | | 2. REPORT TYPE | | 3. DATES COVERED (From — To) | | |
| 16-06-2011 | | Graduate Research Project | | 18 June 2010 — 16 June 2011 | | |
| 4. TITLE AND SUBTITLE Emerging Roles of Combat Communication Units in Cyber Warfare as Related to Computer Network Attack, Defense and Exploitation | | | | 5a. CONTRACT NUMBER | | |
| | | | | N/A | | |
| | | | | 5b. GRANT NUMBER | | |
| | | | | N/A | | |
| | | | | 5c. PROGRAM ELEMENT NUMBER | | |
| | | | | N/A | | |
| 6. AUTHOR(S) Michael J. Myers, Maj, USAF | | | | 5d. PROJECT NUMBER | | |
| | | | | N/A | | |
| | | | | 5e. TASK NUMBER | | |
| | | | | N/A | | |
| | | | | 5f. WORK UNIT NUMBER | | |
| | | | | N/A | | |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) | | | | 8. PERFORMING ORGANIZATION REPORT NUMBER | | |
| Air Force Institute of Technology Graduate School of Engineering and Management 2950 Hobson Way WPAFB OH 45433-7765 | | | | AFIT/ICW/ENG/11-10 | | |
| 9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) | | | | 10. SPONSOR/MONITOR'S ACRONYM(S) | | |
| 689th Combat Communications Wing Commander Col Theresa Giorlando, USAF 575 Tenth Street, Suite 103 Robins AFB, GA 31098-2336 (478)-222-8689 (DSN 472-8689) Theresa.Giorlando@robins.af.mil | | | | 689 CCW/CC | | |
| | | | | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) | | |
| | | | | N/A | | |
| 12. DISTRIBUTION / AVAILABILITY STATEMENT | | | | | | |
| Approval for public release; distribution is unlimited. | | | | | | |
| 13. SUPPLEMENTARY NOTES | | | | | | |
| This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States. | | | | | | |
| 14. ABSTRACT | | | | | | |
| <p>The warfighter has become increasingly dependent of the cyber domain and the computer network that all the deployed forces use to plan and execute the Commander's intent and accomplish the objectives for mission success. The full spectrum of cyber dominance must include the need for computer network attack, defense and exploitation (CNA/D/E) at the tactical level. The combat communications squadrons (CCS) are the Air Force's deployable communication force structure for the joint and coalition warfighter during combat and Humanitarian Relief Operations. With the growing intensity to defend the warfighter's mission that is dependent on the network, instead of defending the entire Air Force GIG, the CCS's core competencies must continue to move from network assurance to mission assurance in a tactical communication environment. In order to provide this complete capability for the warfighter, the combat communication squadrons should reshape their mission to include the cyber operations focus of CNA/D/E. The CCS mission should strive to balance bare-base operations with the CNA/D/E capabilities and evolve combat communication squadrons into a total cyber force tactical unit. Therefore, it only makes sense that mission assurance at the lowest possible denominator must be achieved and maintained. This research intends to show how an Air Force CCS can provide those complete cyber capabilities needed for a deployed force commander to obtain full mission assurance in the cyber domain through a new CCS team structure and time-phased implementation plan.</p> | | | | | | |
| 15. SUBJECT TERMS | | | | | | |
| Combat Tactical Communications, Computer Network Attack, Defense, Exploitation, Mission & Network Assurance | | | | | | |
| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON | |
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | Dr. Michael Grimaila Michael.Grimaila@afit.edu | |
| U | U | U | UU | 91 | 19b. TELEPHONE NUMBER (include area code) | |
| | | | | | | (937) 255-3636, ext 4527 |